FortiOS Handbook

What's New for FortiOS 5.2

FortiOS Handbook - What's New for FortiOS 5.2

September 5, 2014

01-502-117003-20140108

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
Video Tutorials	video.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
September 5, 2014	Added “New features in FortiOS 5.2 Patch 1” on page 13
July 2, 2014	Corrected “DHCP and PPPOE Support for Active-Passive Mode” on page 102.
June 16, 2014	Corrected and added information to “SSL/Deep Inspection Exemptions” on page 64. Added “Flash-based Logging Disabled on Some Models” on page 114.
June 13, 2014	Initial Release

Introduction

This document lists and describes many of the new features added to FortiOS 5.2.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:

- New features in FortiOS 5.2 Patch 1 provides a brief description of features that were added to Patch 1 of FortiOS 5.2.
- Top Features described some of the most important new features in FortiOS 5.2.
- System Features contains information on features connected to global settings.
- Usability Enhancements describes some enhancements that make the web-based manager easier to use and more effective.
- The next sections deal with new features for specific areas of network configuration:
  - Firewall
  - Security Profiles
  - IPsec VPN
  - SSL VPN
  - Authentication
  - Managing Devices
  - Wireless Networking
  - IPv6
  - High Availability
  - WAN Optimization, Web Cache, and Explicit Proxy
  - Advanced Routing
  - Logging and Reporting
- Other New Features contains information about other features that have been added in FortiOS 5.2.
- RFC List contains information about RFCs that are supported by the new features.

New features in FortiOS 5.2 Patch 1

This chapter provides a brief introduction to the following features that were added to Patch 1 of FortiOS 5.2. See the release notes for a complete list of new features/resolved issues in this release.

- Include bandwidth and setup rate statistics in the event log
- Allow export of collected emails
- Ssl-ssh-profile is no longer mandatory when utm profiles are enabled
- Disallow multiple destination interfaces on an IPsec firewall policy
- Add a new diag test command for fnbamd
- Add deregister all option in diagnose endpoint control registration
- Redirect kernel messages to non-console terminals
- Add FortiExtender supported 3G/4G modem list
- Add a new option for STP forwarding
- Suppress probe response based on threshold in wireless controller vap
- Move global antivirus service settings into profile-protocol-options
- Add Ekahau Blink Protocol support and reorganization for station-locate
- Implement diagnose command to test flash SSD
- Online help improvements
- Add iprope check trace in flow trace
- Log id-fields reference improvements
- Add diagnose debug admin error-log command
- Improve hasync debug
- Improve interface list and switch mode
- Wizard improvement
- Allow VIP with port forwarding to permit ICMP
- Support captive portal for block notification page
- Add diagnose log clear-kernel-state command
- Apply new LDAP Tree Browser design to the User Wizard and User Group page
- New Join and try requests to FortiCloud for low-end models

Include bandwidth and setup rate statistics in the event log

Bandwidth and setup rate statistics are vital for customer's units health reports.

The advantage of these parameters are:

- Improves performance on FAZ. Simple query small logs makes FAZ build reports faster and have more idle time for other reports.
- Reduces amount of logs send to FAZ.
- Uses less disk space on FAZ for the same report type.

Allow export of collected emails

This feature adds a new monitor page called *Collected Email Addresses* under *User & Device* > *Monitor* menu, it is essentially a filter on the device list for devices that have an email address associated with them.

The feature allows the administrator to export the list to a CSV file which can then be used for marketing or analysis purposes.

Ssl-ssh-profile is no longer mandatory when utm profiles are enabled

When UTM profiles are enabled in a security policy, you can set or unset `ssl-ssh profile`.

Syntax

```
config firewall policy
  edit 1
    set ssl-ssh profile <test>
  next
end
```

Disallow multiple destination interfaces on an IPsec firewall policy

When a firewall policy is set to action *IPsec*, multiple *Outgoing Interface* should not be allowed.

Since multiple destination interfaces on an IPsec policy aren't necessary, the CLI and GUI was updated to explicitly disallow it.

Add a new diag test command for fnbamd

The following command was added to show authentication session statistics:

Syntax

```
diagnose test application fnbamd 1
```

Sample output

```
diagnose test application  fnbamd  1
Pending sessions:       0
Max session reached:    0
Auth:
    requests:           5000
    sessions:           5000
    released:           5000
Acct:
    requests:           74
    sessions:           0
    released:           0
```

```
Cert:
    requests:           0
    sessions:           0
    released:           0
```

Add deregister all option in diagnose endpoint control registration

When there is a long list of registered endpoint needed to be deregistered, the following command was added to do so:

```
diagnose endpoint registration deregister all
```

Redirect kernel messages to non-console terminals

To be able to see kernel messages from ssh or telnet which needed when customer unit is accessible remotely, the following command has been added:

```
diagnose debug application kmiglogd <Integer>
```

`<Integer>` is the debug level. For example, 1 would be the maximum log level in kernel to be shown.

Add FortiExtender supported 3G/4G modem list

A new 3G/4G modem list is introduced that contain the list of supported modems for both FortiGate and FortiExtender.

GUI changes

Under the *System* > *Network* > *Modem* page, click *Configure Modem* link under the *External Modem* section to see the list for FortiGate and FortiExtender.

Under the *System* > *Network* > *FortiExtender* page, click *Configure Settings* and click *Supported Modems* link under *Modem Settings* section to show the supported FortiExtender modem list. This will jump back to the page under *System* > *Network* > *Modem* page, click *Configure Modem* link.

Syntax

The following new diagnose command was added to show the list of supported FortiExtender modems:

```
diagnose extender modem-list
```

Add a new option for STP forwarding

Due to STP forwarding problem in one-arm transparent mode firewall, a new option: replace nothing (`rpl-nothing`) has been added when configuring `stpforward-mode`.

Syntax

```
config system interface
  edit wan1
    set stpforward enable
    set stpforward-mode rpl-nothing
  next
end
```

Suppress probe response based on threshold in wireless controller vap

The wireless controller vap supports probe response suppression (`probe-resp-suppression`) and probe response threshold (`probe-resp-threshold`).

Syntax

```
config wireless-controller vap
  edit "SSID"
    set probe-resp-suppression enable|disable
    set probe-resp-threshold <value>
  next
end
```

`probe-resp-threshold` range is [-20,-95]dBm, and the default is -80dBm if enabled

Move global antivirus service settings into profile-protocol-options

The global antivirus service settings moved into profile-protocol-options (options included: `uncompsizelimit`, `uncompnestlimit`, `scan-bzip2`, and `block-page-status-code`). HTTP and HTTPS combined into HTTP, `uncompsizelimit` changed to `uncompressed-oversize-limit` and `uncompnestlimit` to `uncompressed-nest-limit`. `scan-bzip2` set to enabled by default and an appropriate help text added.

On upgrade, the options from antivirus service are moved into the corresponding entries in each profile-protocol-options.

CLI changes

The following options are moved from global antivirus service to firewall profile-protocol-options: `uncompsizelimit`, `uncompnestlimit`, `scan-bzip2`, and `block-page-status-code moved`.

The following options are removed: `ftp`, `ftps`, `http`, `https`, `imap`, `imaps`, `nntp`, `pop3`, `pop3s`, `smtp`, and `smtps`.

The following help test was added:

`uncompressed-oversize-limit` Maximum in-memory uncompressed size that can be scanned.

`uncompressed-nest-limit` Maximum uncompress nest level that can be scanned.

`scan-bzip2 Enable/disable` scanning of BZip2 compressed files.

`block-page-status-code` Return code of blocked HTTP pages (non-FortiGuard only).

Add Ekahau Blink Protocol support and reorganization for station-locate

We used to have a config command to report station position for retail analytic server under `config wireless-controller wtp-profile` > `radio` > `station-locate`. A new feature `ekahua-blink-mode` has been added.

These features are all location based service (`LBS`) related and they moved to a sub-config under `wtp-profile`, and they are per `wtp-profile` configuration.

On upgrade, the options from antivirus service are moved into the corresponding entries in each profile-protocol-options.

Syntax

```
config wireless-controller wtp-profile
  edit <wtp-profile-name>
    config lbs
      set ekahau-blink-mode Enable/disable
      set ekahau-tag <xx:xx:xx:xx:xx:xx>
      set erc-server-ip <any_ip>
      set erc-server-port <integer>
    end
  end
```

`<xx:xx:xx:xx:xx:xx>` mac address.

`<any_ip>` Any ip xxx.xxx.xxx.xxx.

`<integer>` input integer value.

Implement diagnose command to test flash SSD

A new diagnose command has been implemented to test the disk.

Syntax

```
diagnose disktest <option>
```

Option can be the following:

`device` Specify which device to test.

`block` The block size of each read/write operation.

`time` The limit of test time of each cycles. Default is no limit.

`size` The limit of test size of each cycles. Default is no limit.

`run` Run test with specified cycles. Default is infinite cycles.

Online help improvements

A video links to some help topics has been added in the FortiOS GUI header bar.

Add iprope check trace in flow trace

Previously flow trace shows only accepted or denied policy information. Sometimes, policy tracking is also important and knowing which policies are checked, and what is the result for the checking might be helpful.

Syntax

`diagnose debug flow show iprope {enable|disable}`

`enable` to enable trace iprope match.

`disable` to disable trace iprope match.

Log id-fields reference improvements

This improvement is to make a complete reference for each log id with its corresponding fields in FortiOS.

CLI changes

Add new `endpoint` and `ha` subcategories into `config log eventfilter`

Syntax

```
config log eventfilter
   set endpoint Enable/disable
   set ha Enable/disable
end
```

GUI changes

Add subtype log filter options named *Endpoint* and *HA* under *Event Log*

Add diagnose debug admin error-log command

Since the last failed admin login is recorded, this new command shows details about the failed admin login attempt.

Syntax

`diagnose debug admin error-log`

Sample output

```
The recent admin user failed login details:
error code      :       -100
method          :       ssh
login name      :       test
cmdb name       :       null
login vdom      :       root
current vdom    :       root
override vdom   :       null
login profile   :       null
```

```
override profile:       null
login time      :       2014-08-29 11:01:57
```

Improve hasync debug

Add diag test application hasync to control hasync debug finely.

Syntax

```
diag test application hasync [1-19,50-53]
```

1 Dump all states of debug switches.

2 Turn off all debug switches.

3 Toggle debug switch of hsync core.

4 Toggle debug switch of ha-diff.

5 Toggle debug switch of FIB.

6 Toggle debug switch of route6.

7 Toggle debug switch of BYOD.

8 Toggle debug switch of endpoint_compliance.

9 Toggle debug switch of NEB.

10 Toggle debug switch of zebos.

11 Toggle debug switch of haconf.

12 Toggle debug switch of proxy.

13 Toggle debug switch of time.

14 Toggle debug switch of snmp.

15 Toggle debug switch of gtp.

16 Toggle debug switch of auth.

17 Toggle debug switch of IPsec.

18 Toggle debug switch of fdb.

19 Toggle debug switch of arp.

50 Dump ha sync statistics.

51 Dump FIB information.

52 Dump extfile's signature.

53 Recalculate external files signature.

Improve interface list and switch mode

This features introduces grouping interfaces by interface type and adds switch to toggle between *VLAN Switch Mode* and regular *Hardware Switch Mode*.

GUI changes

- A *Group By Type* toggle switch has been added in the *interfaces* page under *System* > *Network* > *Interfaces*.
- A *VLAN Switch Mode* toggle switch has been added in the *interfaces* page under *System* > *Network* > *Interfaces*. This *VLAN Switch Mode* toggle switch shows a confirmation dialog when clicked before toggling the system setting.
- A mini faceplate for *Hardware Switch Mode* and *VLAN Switch Mode* has been added in the *member* column under *System* > *Network* > *Interfaces*.

Wizard improvement

The Wizard has been improved to provide instruction page to explain how to set up FortiClient for IPsec and SSLVPN and permit to set up FortiCloud connection on Wizard so that logs will be sent to FortiCloud.

GUI changes

- Add instruction module to generate page explaining how to set up FortiClient for IPsec and SSLVPN depending on the VPN that is configured.
- Add a Wizard Summary Page.
- Allow FortiOS Setup wizard to set up FortiCloud.

Allow VIP with port forwarding to permit ICMP

When a VIP is defined with port forwarding enabled, ICMP (PING) to the mapped IP can be allowed.

Syntax

```
config firewall vip
   edit "VIP"
      set extip xxx.xxx.xxx.xxx
      set extintf "wan1"
      set portforward enable
      set mappedip xxx.xxx.xxx.xxx
      set protocol icmp
   next
end
```

The command `set protocol` has `icmp` option now to make the firewall forward ICMP to the host specified by `mappedip` while the `mappedport` and `extport` attributes are skipped.

Support captive portal for block notification page

The main requirement of this feature is to present a block notification page if the web access is denied by a firewall policy.

Add diagnose log clear-kernel-state command

This command has been added to clear log statistics in kernel in order to improve disk log session setup rate.

Syntax

```
diagnose log clear-kernel-stats
```

Apply new LDAP Tree Browser design to the User Wizard and User Group page

Previously, the LDAP browser shows LDAP containers and LDAP entries within the same tree. When there are many LDAP entries available, it becomes harder for users to select, filter, search different types of LDAP objects.

This new feature now divides the LDAP Browser into two major parts:

- A tree to show the container.
- Tables to show different type of LDAP object entries.

New Join and try requests to FortiCloud for low-end models

These new `join` and `try` requests are for low-end models only such as: FG-30D, FWF-30D, FG-60D, FWF-60D, FG-70D, FG-80D, FG-90D, and FWF-90D.

Syntax

```
exec fortiguard-log join
exec fortiguard-log try <FortiCloud_id> <Password>
```

Top Features

This chapter introduces the following top features of FortiOS 5.2:

- Unified Policy Management
- FortiView Dashboards
- SSL Inspection
- Web Filtering
- Application Control
- IPsec VPN Creation Wizard
- Captive Portal
- FortiAP Management
- Flow-based Antivirus
- FortiExtender Support
- Using a Virtual WAN Link for Redundant Internet Connections
- Internet Key Exchange (IKE)
- SSL VPN Creation
- On-Net Status for FortiClient Devices

Unified Policy Management

The different creation pages in the web-based manager for policy types and subtypes (user-identity, device identity, and VPN) have been merged into a single main policy creation page. New fields have been added for *Source User(s)* and *Source Device Type* that remove the need for multiple authentication rules in a single police. This allows for greater control and customization of policies, as a combination of these source types can be used in a single policy rather than having to pick one type.

For more information, see "Unified Policy Management" on page 55.

FortiView Dashboards

The *FortiView* dashboards integrate real time and historical dashboards into a single view that displays the top 100 sessions on a FortiGate unit. The different dashboards show information on the following:

- Sources
- Applications
- Cloud applications
- Destinations
- Web sites
- Threats
- All sessions

For more information, see "FortiView Dashboards" on page 43.

SSL Inspection

Several changes have been made to how SSL inspection is handled by a FortiGate unit, with the addition of a new mode that allowed HTTPS traffic to be scanned without enabling deep inspection, as well as changes to the handling of certificates and configuring exemptions for SSL inspection.

For more information, see "SSL Inspection" on page 64.

Web Filtering

Several new options have been added for web filtering:

- Restricting Google access to specific domains
- New protocols for warnings and authentication
- Modifying HTTP request headers
- Adding a referer to URL filters.
- Using FortiGuard rating checks for images, JavaScript, CSS, and CRL
- Additional replacement message variables

For more information, see "Web Filtering" on page 66.

Application Control

Several new options have been added for application control:

- Deep inspection for cloud applications
- Traffic shaping settings
- 5-Point-Risk Ratings
- Replacement messages
- Support for SPDY protocol

For more information, see "Application Control" on page 70.

IPsec VPN Creation Wizard

The IPsec VPN wizard is the only web-based manager tool for creating interface- or route-based IPsec VPNs. All it takes is a few steps with the wizard to create a wide variety of interface-based IPsec VPN configurations. In addition to the IPsec settings the wizard creates all required routes and policies.

In FortiOS 5.2, expanded options have been added to the wizard, allowing it to be used for more types of VPN configurations. Tunnel templates have been created for popular configurations.

For more information, see "VPN Creation Wizard" on page 76.

Captive Portal

Several new options have been added for captive portals:

- External captive portals
- Using groups from the security policy
- Exempting a policy
- Replacement messages
- New configuration options for wireless
- WPA personal security + captive portal for wireless

For more information, see "Captive Portal" on page 88 and "Captive Portal for WiFi" on page 96.

FortiAP Management

Several new options have been added for managing FortiAP units:

- Manually selecting AP profiles
- AP scanning
- Radio settings summary
- CLI console access
- Split tunneling for wireless traffic

For more information, see "FortiAP Management" on page 94.

Flow-based Antivirus

In FortiOS 5.2, flow-based AntiVirus has been improved to have the same enhanced performance as flow-based antivirus scanning in FortiOS 5.0 while providing the same accuracy and many of the extended features of proxy-based antivirus.

For more information, see "Flow-based Antivirus" on page 72.

FortiExtender Support

FortiOS 5.2 supports FortiExtender, that allows you to remotely connect 4G/LTE USB modems to a FortiGate unit. The FortiGate unit can remained installed in a secure location while the FortiExtender is installed on a roof or near a window providing enhanced 4G/LTE modem reception.

For more information, see "FortiExtender Support" on page 26.

Using a Virtual WAN Link for Redundant Internet Connections

A virtual WAN link consists of two or more interfaces that are connected to multiple ISPs. The FortiGate unit sees the virtual WAN link as a single interface so the FortiGate's security policy configuration no longer has be redundant to support dual Internet links. In addition, the virtual WAN link includes load balancing and new link health checking and settings.

For more information, see “Using a Virtual WAN Link for Redundant Internet Connections” on page 28.

Internet Key Exchange (IKE)

Several new options have been added for how IKE is supported on a FortiGate:

- Multiple interfaces
- Mode-configuration
- Certificates groups
- Authentication methods
- Inheriting groups from the security policy
- Assigning client IP addresses using the DHCP proxy
- Transform matching
- Cookie notification
- Message ID sync for High Availability

For more information, see “Internet Key Exchange (IKE)” on page 77.

SSL VPN Creation

SSL VPN configuration has been simplified with new settings and portal creation pages. Most SSL VPN settings can be configured on one web-based manager page, with additional settings handled as part of the security policy.

For more information, see “SSL VPN Configuration” on page 86.

On-Net Status for FortiClient Devices

A new status option, On-Net, has been added for FortiClient devices that show if that device has been registered with the FortiGate unit.

For more information, see “On-Net Status for FortiClient Devices” on page 92.

System Features

New system features include:

FortiExtender Support

FortiOS 5.2 supports the new FortiExtender unit, which provides internet connectivity via 4G/LTE network to a FortiGate unit.

To connect a FortiGate and FortiExtender, a new tap interface is created on the FortiGate unit, which receives the IP address from the cellular service provider via the FortiExtender, using a CAPWAP data channel. All the packets sent to the tap interface are received by the extender module on the FortiGate and are then sent to the FortiExtender, which then sends the packets out on the 4G/LTE network.

When data packets are received from the cellular network, the FortiExtender passes the packets to the FortiGate via the CAPWAP data channel. These packets are written to the tap interface and the FortiGate IP stack will process them.

The options to configure a FortiExtender unit can be found by going to *System* > *Network* > *FortiExtender*.

The configuration of a FortiExtender interface is restricted to the root VDOM.

Connecting a FortiExtender unit to a FortiGate unit

1. If you are using the provided PoE injector:
   a. Plug the provided Ethernet cable into the Ethernet port of the FortiExtender and insert the other end of the Ethernet cable into the AP/Bridge port on the injector, then plug the injector into an electrical outlet.
   b. Connect the LAN port of the PoE injector to a FortiGate, FortiWifi, or FortiSwitch device.
2. If you are not using the PoE injector, insert the other end of the Ethernet cable into a PoE LAN port on an appropriate FortiGate, FortiWiFi or FortiSwitch device.

   For more information on connecting the FortiExtender unit, see the *QuickStart Guide*.
3. By default, the options for the FortiExtender are hidden and disabled. Enable them in FortiGate's CLI:

```
config system global
  set fortiextender enable
  set wireless-controller enable
end
```

4. Enable the control and provisioning of Wireless Access Point (CAPWAP) service on the port to which the FortiExtender unit is connected (*lan* interface in this example) using the following CLI commands:

```
config system interface
  edit lan
    set allowaccess capwap
  end
end
```

   Once enabled, it appears as a virtual WAN interface in the FortiGate, such as *fext-wan1.*

Configuring the FortiExtender unit

1. At this point, you can fully manage the FortiExtender from the FortiGate unit. To achieve this, you need to authorize the FortiExtender by going to *System* > *Network* > *FortiExtender* and click on *Authorize.* Once authorized, you can configure the following settings as required:
   - *Link Status*: Shows you if the link is *Up* or *Down,* click on *Details* to see the System and Modem Status.
   - *IP Address*: Shows you the current FortiExtender's IP address, click on the link of the IP address to connect to the FortiExtender GUI.
   - *OS Version:* Shows the current FortiExtender's build, click on *Upgrade* if you wish to upgrade the Firmware.
   - *Configure Settings*: Allows you to configure the Modem Settings (for more information, see below), PPP Authentication, General, GSM / LTE, and CDMA .
   - *Diagnostics*: Allows you to diagnose the FortiExtender unit, you can choose a command form the existing commands and click on *Run.* Existing commands are: `Show device info, Show data session connection status, test connection, test disconnection, Get signal strength, AT Command.`

The FortiExtender unit allows for two modes of operation for the modem; *On Demand* and *Always Connect*. In *On Demand* mode, the modem connects to a dialup ISP account to provide the connection to the Internet when needed. In *Always Connect* mode, the modem is always connected to the internet, it can acts as a primary or backup method of connecting to the Internet. To configure the dial mode as needed, do the following:

2. Select *Configure Settings*.
3. Extend *Modem Settings*.
4. Select the *Dial Mode* of *Always Connect* or *On Demand*.
5. Enter the *Quota Limit* to the desired limit in Mega Byte.
6. Select *OK*.

Configuring the FortiGate unit

1. Go to *Router* > *Static* > *Static Routes* or *System* > *Network* > *Routing*, depending on your FortiGate model, and select *Create New*.

If your network will be using IPv6 addresses, go to *Router* > *Static* > *Static Routes* or *System* > *Network* > *Routing* and select *IPv6 Route*.

2. Set the *Destination IP/Mask* to 0.0.0.0/0.0.0.0, *Device* to *fext-wan1*, and set the *Gateway* to your gateway IP or to the next hop router, depending on your network requirements.
3. Select *OK.*
4. Go to *Policy & Objects* > *Policy* > *IPv4* and select *Create New.*

If your network will be using IPv6 addresses, go to *Policy & Objects* > *Policy* > *IPv6* and select *Create New.*

5. Set the *Incoming Interface* to the internal interface and the *Outgoing Interface* to *fext-wan1* interface. You will also need to set *Source Address*, *Destination Address*, *Schedule*, and *Service* according to your network requirements.
6. Make sure the *Action* is set to *ACCEPT*. Turn on *NAT* and make sure *Use Destination Interface Address* is selected.
7. Select *OK.*

Using a Virtual WAN Link for Redundant Internet Connections

To make sure your network is always connected to the Internet you can engage the services of two or more Internet service providers and set up redundant Internet connections. Then, if one of your ISPs service is interrupted, all of your Internet traffic can be switched to the other ISP, maintaining your Internet connection. Also, while both ISPs are operating you can load balance traffic between them, increasing your network's available Internet bandwidth.

Previous versions of FortiOS required a few steps to set up two interfaces as redundant Internet connections. The setup also involved some special routing and load balancing setup and creating duplicate policy configurations for each Internet facing interface. In addition, previous versions of FortiOS supported basic link monitoring.

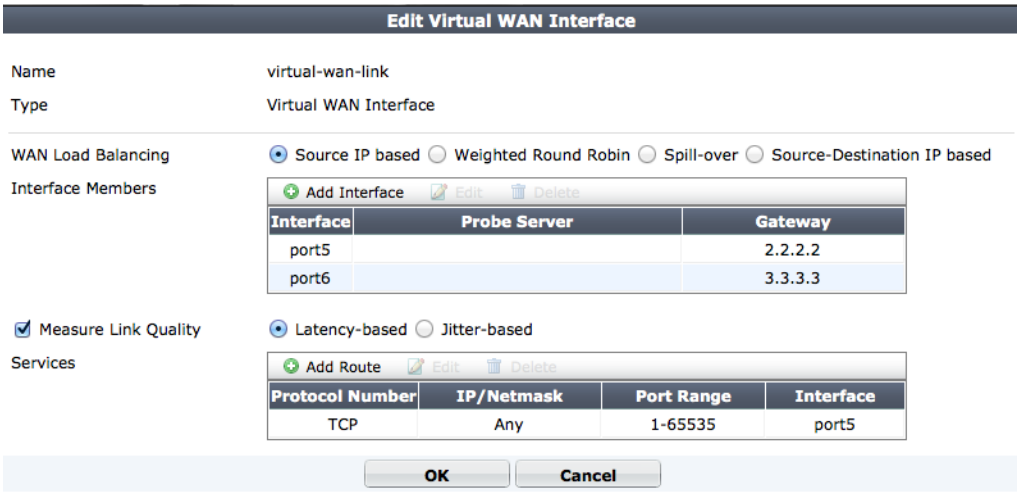
FortiOS 5.2 adds a new type of interface called a virtual WAN link. A virtual WAN link consists of two or more physical interfaces that are connected to two or more ISPs and to the Internet as well as the load balancing and routing configuration required to support redundant internet connections. In addition, the virtual WAN link configuration also includes new link health checking and settings to control traffic flow based on link health.

The FortiGate unit sees the virtual WAN link as a single interface so the FortiGate's security policy configuration no longer has be redundant to support dual Internet links. Now one policy configuration to control traffic to the virtual WAN link is all that is required. You can also add or remove redundant Internet links just by adding or removing physical interfaces from the virtual WAN link. No addition changes to the routing, load balancing or firewall policy configuration are required.

Setting Up a Virtual WAN Link

To set up a virtual WAN link, go to *System* > *Network* > *Interfaces* and select *Create New* > *Virtual WAN*. Add the interfaces connected to ISPs to the virtual WAN link. For each interface you must enter a gateway IP, usually provided by your ISP. You can also change load balancing settings (such as Spillover Threshold and Weight) and set up link health checking (called measuring link quality).

Figure 1: Virtual WAN link configuration



Once you have added interfaces to the virtual WAN interface you should go to *Router* > *Static* > *Static Route* and add a default route for the virtual WAN link. Then add firewall policies that allow access to the Internet by setting the outgoing interface to virtual-wan-link.

For more information about using a virtual WAN link, please see the FortiGate Cookbook recipe *Using a virtual WAN link for redundant Internet connections*, found at docs.fortinet.com.

Setting Up Virtual WAN Link Load Balancing

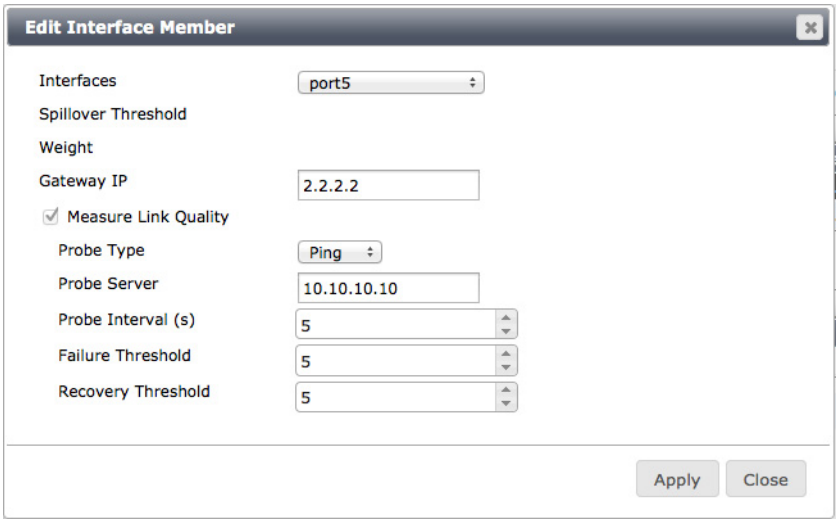
By default when you set up a virtual WAN link source IP based load balancing is selected and traffic is load balanced among the interfaces added to virtual WAN link configuration. You can change the load balancing method to weighted load balancing, spill-over load balancing or source-destination IP load balancing. Selecting a different load balancing method may also require configuring the interfaces added to the virtual WAN link to add weights (for weighted load balancing) or to set spillover thresholds.

Directing Traffic to Higher Quality Links

You can configure link quality measuring (link health checking) on the interfaces added to the virtual WAN link. Depending on how you configure the virtual WAN link this link quality checking is based on latency or jitter. With link quality checking in place you can configure Services to control the links used for selected types of traffic. For example, media-based traffic like SIP is very sensitive to jitter. If you set up link quality checking to check for jitter, you can configure the virtual WAN link to send SIP traffic to the link with the lowest jitter (and so the highest quality link).

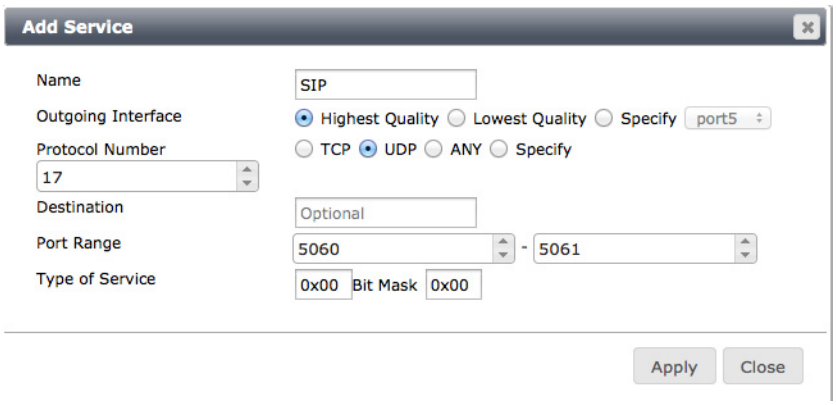
To configure link checking on individual interfaces added to a virtual WAN link, edit Interface members in the virtual WAN link, select Measure Link Quality and set the quality measurement options. You can measure link quality using ping or HTTP, select a server to communicate with to perform link quality checking and set the probe interval, failure threshold and recovery threshold.

Figure 2: Configuring link health checking



Next, add Services that control how traffic patterns are affected by link quality. Services work like policy routes. Configure a service by defining a traffic type (for example, SIP) and specifying whether this traffic always goes to the highest quality interface, the lowest quality interface or a specific interface no matter the quality.

Figure 3: Virtual WAN link service



Measured Volume Based Distribution

Your FortiGate can actively measure the volume of traffic sent to each WAN link and distribute new sessions to balance the traffic volume to each link using a simple ratio calculation. To use this feature, use the following CLI command:

```
config system virtual-wan-link
  set load-balance-mode measured-volume-based
  config member
    edit <ID>
      set volume-ratio <number>
    end
  end
end
```

The Link Monitor

You can monitor link health using the *Link* monitor, which can be found by going to *System* > *Monitor* > *Link Monitor*.

FortiGuard Services

Several changes have been made to how FortiGuard services can be received by your FortiGate unit.

Updates from Multiple FortiManager Units

In FortiOS 5.2, you can configure your FortiGate unit to check with up to three FortiManagers for FortiGuard signature updates, and use another set of up to three FortiManagers for FortiGuard web filtering URL lookups.

Syntax

Use the following command to configure your FortiGate unit with the addresses of three FortiManagers that the FortiGate will use to get FortiGuard signature updates:

```
config system central-management
  set fortimanager-fds-sigupdate-override enable
  set sig-update-server-1 10.10.10.10
  set sig-update-server-2 20.20.20.20
  set sig-update-server-3 30.30.30.30
end
```

When the FortiGate unit checks for signature updates it attempts to connect to update server 1. If the connection fails it tries update server 2 then 3. It connects to the first one that's available to get updates.

Use the following command to configure your FortiGate unit with the addresses of three FortiManagers that the FortiGate will use for FortiGuard Web Filtering URL lookups:

```
config system central-management
  set fortimanager-fds-urllookup-override enable
  set url-lookup-server-1 11.11.11.11
  set url-lookup-server-2 12.12.12.12
  set url-lookup-server-3 13.13.13.13
end
```

When the FortiGate unit needs to do a web filtering lookup it attempts to connect to lookup server 1. If the connection fails it tries lookup server 2 then 3. It connects to the first one that's available to do the lookup.

FortiGuard Server List

In FortiOS 5.2, you can create a server list for receiving FortiGuard updates, allowing you to use different servers for different FortiGuard services. Each server can be used for either web filter and anti-spam ratings or AV/IPS signature updates.

The server list also has the ability to include the default servers by adding them to the end of the list. This option is only available if the central management type is not set to FortiGuard.

If no server list is configured, the FortiGuard will not use the public FortiGuard servers as resolved by DNS.

Syntax

```
config server-list
  edit <ID>
    set server-type {rating | update}
    set server-address <address>
  end
  set include-default-servers {enable | disable}
end
```

Using TCP Port 80 to Receive Updates from a FortiManager Unit

Communications to a FortiManager unit in order to receive FortiGuard updates are now supported using TCP port 80.

To configure communications to use port 80, go to *System* > *Config* > *FortiGuard* and expand *Web Filtering and Email Filtering Options*. Select *Use Alternate Port (80)*. This can also be configured using the CLI.

Syntax

```
config system fortiguard
  set port 80
end
```

FortiGuard TCP stats can also be displayed using the `diagnose test application urlfilter 20` command.

Netflow v9.0

FortiOS 5.2 supports Netflow v9.0. NetFlow services provide network administrators with access to IP flow information from their data networks. Network elements (routers and switches) gather flow data and export it to collectors. The collected data provides fine-grained metering for highly flexible and detailed resource usage accounting.

A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device. These collected flows are exported to an external device, the NetFlow collector. Network flow records include details such as IP addresses, packet and byte counts, timestamps, application ports, and input and output interfaces.

Configuring the Global Settings for Netflow Collector and Timers

The global settings for Netflow can be configured in the CLI:

```
config system netflow
   set collector-ip <address>
   set collector-port <port>
   set source-ip <address>
   set active-flow-timeout <integer>
   set inactive-flow-timeout <integer>
end
```

The value for `active-flow-timeout` is used as the minimum length of a live session, as well as for the intervals to send the report. The default is 1 minute, meaning that if a session lives for a minute, it will be reported in a Netflow packet.

The value for `inactive-flow-timeout` is used as the interval to send a Netflow report of inactive (finished) flows. Since FortiOS uses 1350 Byte payloads, the number of reports in a packet are limited and multiple packets may be sent regardless of this timer.

Using Netflow with VDOMs

For VDOM environments, excluding the management VDOM, Netflow must be configured using the following CLI commands:

```
config system vdom-netflow
   set vdom-netflow enable
   set collector-ip <address>
   set collector-port <port>
   set source-ip <address>
end
```

Adding Netflow Sampling to an Interface

Netflow sampling can be enabled on an interface to sample transmitted traffic (tx), received traffic (rx), or both using the CLI:

```
config system interface
   edit <name>
      set netflow-sampler {disable | tx | rx | both}
   end
end
```

Viewing the Configuration

Netflow does not have a separate daemon and is instead running under sflowd. The current Netflow configuration can be viewed by using test level 3 or 4:

```
diagnose test application sflowd 3
```

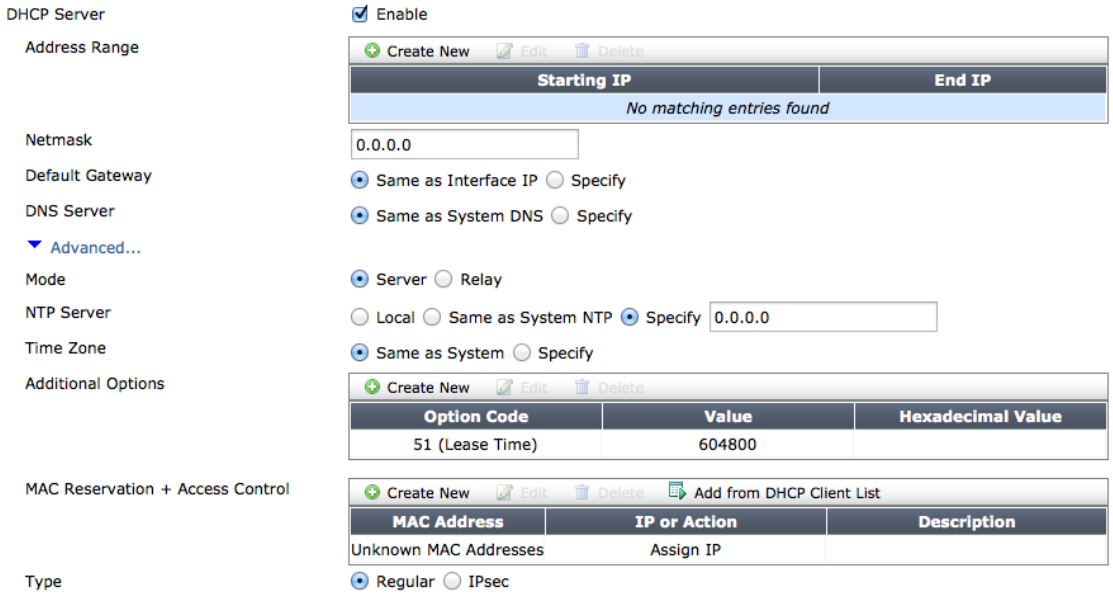
```
diagnose test application sflowd 4
```

DHCP Server Configuration

The following attributes have been added for DHCP server configuration to both the web-based manager and the CLI:

- Time zone
- TFTP server
- TFTP filename

Figure 4: DCHP server settings



Syntax

```
config system dhcp server
   edit <integer>
      set timezone-option {disable | default | specify}
      set timezone <timezone_code>
      set tftp-server <string>
      set filename <file_name>
      end
end
```

Improvements to Aggregate/Redundant Interfaces

Several improvements have been made in FortiOS 5.2 for aggregate or redundant interfaces.

Minimum Number of Links in an Aggregation

You can now set a minimum number of links that must exist in an aggregation. If this number is not reached, the device will failover. The minimum links value can be set between 1-32, with 1 being the default value.

Aggregates can also now be configured so that they are taken down administratively when the min-links threshold is passed. This will cause all the members to be taken down administratively as well.

Syntax

```
config system interface
  edit <name>
    set type aggregate
    set vdom root
    set member <ports>
    set min-links <integer>
    set min-links-down administrative
  end
end
```

Avoiding Traffic Disturbances

Two new methods have been added to avoid traffic disturbances for an aggregate that can be caused by ports flapping up and down and being repeatedly added and removed from the aggregate.

Setting the Link Up Delay Period

When a member port in an aggregate/redundant becomes operationally up, be default it is considered as a viable port for aggregation/redundancy after 50ms. Increasing this delay can minimizing the effect of a flapping port by causing the FortiGate to wait longer before deciding if a port is considered viable. This option is available for both redundant and aggregate interfaces.

Syntax

```
config system interface
  edit <name>
    set type {aggregate | redundant}
    set link-up-delay <time>
  end
end
```

Enabling Priority Override

In the case of a redundant port, there is only one port actively carrying traffic thus the only time a port coming up can affect existing traffic is where the primary port went down, traffic moved to a secondary and then the primary came back up. In this case since there is only one port the impact of switching ports is more noticeable and thus it may be desirable to not switch back to the original primary just because it is up. Instead traffic should only switch back if the currently active secondary fails.

To support that, the command `set priority-override` has been added for redundant interfaces. If `priority-override` is enabled, then when a port with a higher priority comes up then traffic switches to it. With `priority-override` disabled, traffic will only switch to a higher priority port if the current port fails.

Syntax

```
config system interface
  edit <name>
    set type redundant
    set priority-override {enable | disable}
  end
end
```

Link Layer Description Protocol

Link Layer Description Protocol (LLDP) is supported in FortiOS 5.2. LLDP allows a device to advertise its existence and capabilities to other devices.

The primary use for LLDP is to improve a FortiGate unit's device detection output when another FortiGate unit is detected. LLDP information is used to populate the device record on the FortiGate unit performing device detection. Any LLDP information transmitted by a peer is ignored unless FortiGate device detection is enabled on an interface. If device detection is enabled, then the subset of LLDP information sent by the peer that is relevant to device detection is shown in the `diagnose user device list` output.

The transmitted LLDP attributes on a given port are:

- Chassis ID
- Port ID
- TTL
- System Name
- System Description
- System Capabilities
- Aggregation
- Host Name

LLDP transmission is enabled by default on all ports that support a MAC address. It can be disabled globally, or disabled on some interfaces or VDOMs, while being enabled on others.

Syntax

To disable LLDP globally or on a specific VDOM, use the following command:

```
config system global
  set lldp-transmission disable
end
```

To enable LLDP at the individual interface level, first disable LLDP globally, then use the following command:

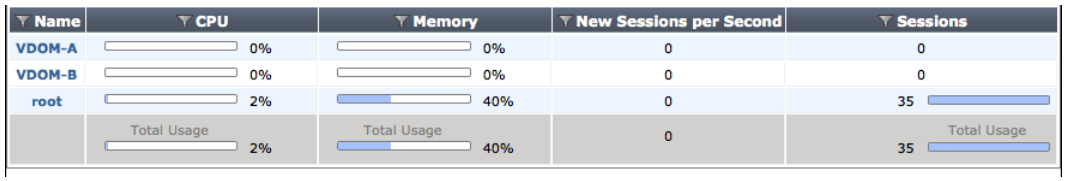
```
config system interface
  edit <name>
    set lldp-transmission enable
  end
end
```

CPU and Memory Usage per VDOM

In FortiOS 5.2, the following information sources are available concerning both CPU and memory usage per VDOM:

- Default columns for CPU and Memory have been added to the VDOM list.
- Optional columns for Sessions and New Sessions per Second have been added to the VDOM list.
- A summary line has been added to at the bottom of the VDOM list to show global CPU, memory, sessions, and sessions per second usage.
- The CLI command `diagnose system vd stats` has been added to display VDOM statistics.

VDOM list



Custom Languages for Guest Management and SSL VPN Portals

Custom language files can now be used for guest management admin accounts, as well as guest portals, SSL VPN portals, and SSL VPN user settings.

To use this feature, it must be enabled in the CLI. Language files can now be managed, imported, and downloaded by going to *System* > *Config* > *Advanced*. Further configuration can be done in the CLI.

Syntax

1. Enabling the feature:

```
config system global
   set gui-custom-language enable
end
```

2. Downloading a custom language file from a TFTP server:

```
execute system custom-language import <lang_name> <file_name>
     <tftp_server_ip>
```

3. Managing custom languages:

```
config system custom-language
   edit <lang_name>
      set filename <file_name>
   end
end
```

4. Setting the custom language for an admin account with `guest-auth` enabled:

```
config system admin
   edit <name>
      set guest-auth enable
      set guest-lang <lang_name>
   end
end
```

5. Setting the custom language for an SSL-VPN portal with `web-mode` enabled:

```
config vpn ssl interface
  edit <name>
    set web-mode enable
    set custom-lang <lang_name>
  end
end
```

6. Setting the custom language for an SSL-VPN user:

```
config vpn ssl web user-bookmark
  edit <name>
    set custom-lang <lang_name>
  end
end
```

Packet Capture Options for Admin Profiles

Packet capture can now be configured in an admin profile and set to *None*, *Read Only*, or *Read-Write*. The packet capture option can be found by going to *System* > *Admin* > *Admin Profiles* and expanding *Firewall Configuration*.

This feature can also be configured in the CLI.

Syntax

```
config system accprofile
  edit <name>
    set fwgrp custom
      config fwgrp-permission
        set packet-capture {read-only | read-write | none}
      end
    end
  end
end
```

FortiCloud Modem List

The supported modem list that can be downloaded from FortiCloud will now include a list of supported modems by FortiOS and the new FortiExtender unit. To support this, the file format of the list changed from plain text to tar ball that contains two files: `modem_list.conf` for the FortiOS list and `modem_list_fex.conf` for the FortiExtender list.

SPAN Support for Hard-Switch Interfaces

The Switch Port Analyzer (SPAN) feature is now available for hardware switch interfaces on FortiGate models with built-in hardware switches (for example, the FortiGate-100D, 140D, and 200D etc.). The SPAN feature (also called port mirroring) allows you to send a copy of the packets received or sent by one interface to another. So, for example, you could send all traffic received by the WAN interface to another interface and connect a sniffer to that other interface to monitor the traffic on the WAN interface.

To enable SPAN on a hardware switch, go to *System* > *Network* > *Interfaces* and edit a hardware switch interface. By default the system may have a hardware switch interface called *lan*. You can also create a new hardware switch interface.

Select the *SPAN* checkbox. Select a source port from which traffic will be mirrored. Select the destination port to which the mirrored traffic is sent. Select to mirror traffic received, traffic sent, or both.

Figure 5: Configuring SPAN

You can also enable SPAN in the CLI:

Syntax

```
config system virtual-switch
  edit <port>
    set span enable
    set span-source-port <port>
    set span-dest-port <port>
    set span-direction {both | Tx | Rx}
  end
end
```

Setting the Service and AC-name in PPOE PADI/PADO Negotiations

The Service and AC name in the PPPoE PADI/PADO negotiation is now configurable. This allows CLI-specified names to encoded, enhancing logic in the handling of various PPPoE server responses, especially in situations where there are multiple Access Concentrator servers in the Point of Presence site.

Syntax

```
edit port1
  set mode pppoe
  set service-name <name>
  set ac-name <name>
end
```

Disabling FortiExplorer, the USB MGMT Port, and the Serial Console

New CLI commands have been added allowing you to disable access for FortiExplorer on Windows and OS X and the USB MGMT port, or for the serial console, FortiExplorer iOS, the USB MGMT port, and 3G/4G MODEM access.

Syntax

1. Disable FortiExplorer on Windows and OS X and the USB MGMT port:

```
config system console
  set fortiexplorer disable
end
```

2. Disable serial console, FortiExplorer iOS, and 3G/4G MODEM access:

```
config system console
  set login disable
end
```

Port Kernel Profiling

Port kernel profiling is now supported in FortiOS 5.2. To use this feature, enter the command `diagnose sys profile` into the CLI. If you press enter, the following options are available:

1. set cpu mask
2. run start command
3. run stop command to read the profiling data and analyze
4. run show command to show the result
5. set cpu mask 00 to stop profiling

The following attributes are also available:

- `cpumask` - profile which CPUs.
- `module` - show kernel module (This is only available when the kernel is module mode).
- `show` - show kernel profiling result.
- `start` - start kernel profiling data.
- `stop` - copy kernel profiling data.
- `sysmap` - show kernel sysmap.

Using a Second Destination IP (VRDST)

VRRP can now be configured with second destination IP (VRDST) for monitoring. When two IPs are used, VRRP failure will only be reported if both monitored IPs are down.

A second VRDST can be configured using the CLI.

Syntax

```
  config system interface
    edit <interface>
      config vrrp
        edit <id>
          set vrdst <ip1> <ip2>
        end
      end
    end
  end
end
```

Session Rate Stats per VDOM

The command `diagnose system vd list` now displays the session setup rate. This feature is supported for both IPv4 and IPv6.

Disable Honoring the Don't-Fragment Flag

Honoring the Don't-Fragment flag can now be disabled through the CLI. This allows the FortiGate unit to fragment the packet as required, even when the Don't-Fragment flag is set.

Syntax

```
config system global
  set honor-df disable
end
```

Disable Login Time Recording

Login time recording, which is enabled by default, can now be disabled using the CLI.

Syntax

```
config system global
  set login-timestamp disable
end
```

Per-IP-Bandwidth-Usage Feature Removed

The Per-IP-Bandwidth feature has been removed in FortiOS 5.2. This includes both the *Per-P-Bandwidth* widget in the web-based manager and all related CLI commands.

Modem Support

The Novatel MC679 and Sierra 313U modems are supported in FortiOS 5.2 for use with a FortiGate unit.

An MIB entry, `fgUsbModemSignalStrength`, has also been added to display modem signal strength.

Usability Enhancements

Many usability enhancements have been made to the web-based manager in FortiOS 5.2, in order to make the configuration process more efficient. New usability enhancements include:

FortiView Dashboards

In order for information to appear in the *FortiView* dashboards, disk logging must be selected for the FortiGate unit. To select disk logging, go to *Log & Report* > *Log Config* > *Log Settings*.

Disk logging is disabled by default for some FortiGate units. To enable disk logging, enter the following command in the CLI:

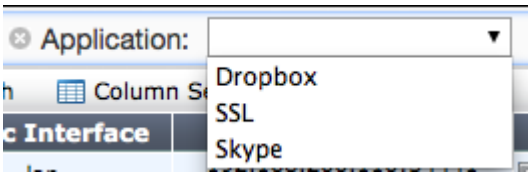
```
config log disk setting
  set status enable
end
```

Please note that flash-based logging has been disabled in FortiOS 5.2 for certain models. To view a complete list of affected models, please refer to the *Release Notes*.

The *FortiView* dashboards integrate real time and historical dashboards into a single view. These dashboards can be found by going to *Status* > *FortiView*. Each dashboard will initially display the top 100 sessions but when the results are filtered, other sessions may be displayed.

Each dashboards can be filtered by a variety of attributes. Attributes can be selected by using the dropdown menu located at the top of each widgets that displays only the options that have results; for example, if the only applications used in the are Dropbox, SSL, and Skype, the only options in the dropdown menu for the Application filter will be Dropbox, SSL, and Skype.

Figure 6: Filtering for Applications



Results can also be filtered using the various columns, although not all columns support this.

The dashboards also include different time options, allowing you to see current traffic in real-time, or historical traffic that occurred in the last 5 minutes, 1 hour, or 24 hours.

Historical traffic is only supported on FortiGate models that have local storage. The 24 hours option is also unavailable for desktop models (FortiGate-90 series and below).

Sources

The *Sources* dashboard shows information about the sources of traffic on your FortiGate unit, including user and device. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by source IP, source device, source interface, destination interface, and policy ID.

Figure 7: The *Sources* dashboard

Source	Device	Sessions	Bytes (Sent/Received)
10.10.80.3	Alais	122	539.94 K
10.10.80.4	Nicola	4	163.12 K
10.10.80.2	Wii	1	386

Applications

The *Applications* dashboard shows information about the applications being used on your network, including application name, category, and risk level. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by application, source interface, destination interface, and policy ID.

In order for information to appear in the *Applications* dashboard, application control must be enabled in a policy.

Figure 8: The *Applications* dashboard

Application	Category	Risk	Sessions	Bytes (Sent/Received)
DNS	Network.Service		35	9.44 K
Skype	P2P		23	589.99 K
Hola.Unblocker	Proxy		21	440.08 K
SMTPS	Email		1	10.46 K
Dropbox	Storage.Backup		1	12.11 K

Cloud Applications

The *Cloud Applications* dashboard shows information about the cloud applications being used on your network, including application name, category, risk level, login IDs, and, if applicable, the number of videos played. If the cursor is held over the column showing the number of videos, the titles of these videos will be shown. Additional columns show information about sessions and bytes sent or received.

Two different views are available for the Cloud Applications dashboard: applications and users. Applications shows a list of the programs being used. Users shows information on the individual users of the cloud applications, including the username if the FortiGate was able to view the login event.

This dashboard can be filtered by application, source interface, destination interface, and policy ID.

In order for information to appear in the *Cloud Applications* dashboard, an application control profile that has *Deep Inspection of Cloud Applications* turned on must be enabled in a policy and SSL Inspection must use `deep-inspection` (for more information, see "SSL Inspection" on page 64).

Figure 9: The *Cloud Applications* dashboard

Application	Category	Risk	Login IDs	Sessions	Files (Up/Down)	Videos Played	Bytes (Sent/Receive
Youtube	Video/Audio		1	25		8	139.77 M
Vimeo	Video/Audio		1	1		1	4.85 M
Dropbox	File.Sharing		1	1	0 / 1		15.09 M

Destinations

The *Destinations* dashboard shows information about the destination IPs of traffic on your FortiGate unit, as well as the application used. Additional columns show information about sessions and bytes sent or received.

This dashboard can be filtered by destination IP, user, source interface, destination interface, and policy ID.

Figure 10: The *Destinations* dashboard

Destination	Applicati...	Sessions	Bytes (Sent/Received)
pongs.blip.tv (54.243.171.49)	Unknown	2	71.42 K
gwb.lphbs.com (199.127.194.181)	Unknown	1	45.33 K
notify3.dropbox.com (108.160.167.157)	Dropbox	1	555
dsn0.d.skype.net (157.55.130.156)	Unknown	1	8.29 K
dsn15.d.skype.net (157.55.56.154)	Unknown	1	3.84 K
104.0.14.6.0.rst6.r.skype.net (157.55.133.145)	Unknown	1	5.03 K

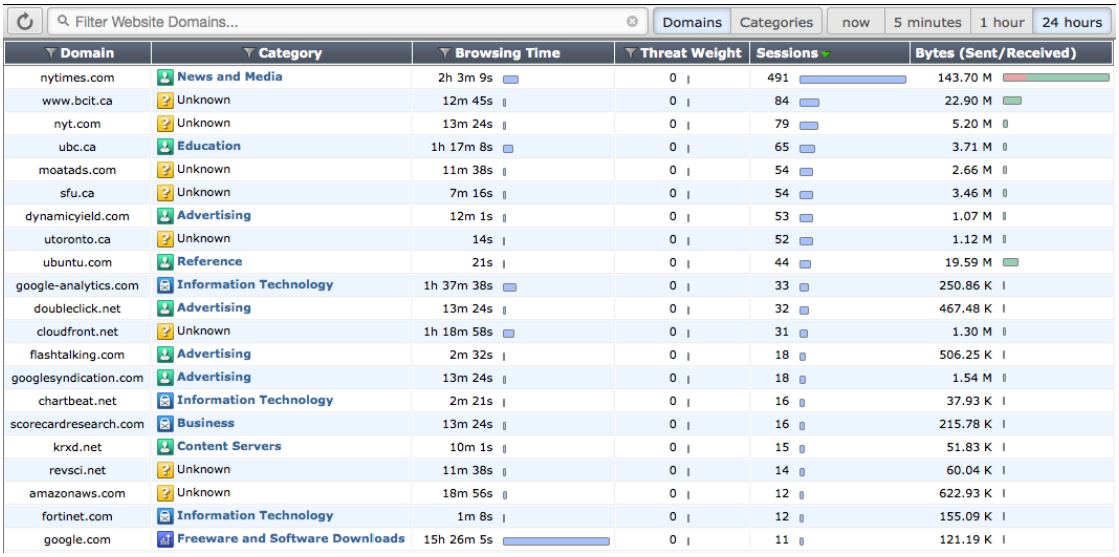
Web Sites

The *Web Sites* dashboard lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be clicked on in order to see a description of the category and several example sites, with content loaded from FortiGuard on demand. New icons have also been added for FortiGuard category groups. Additional information is provided about domain, browsing time, threat weight, sources, and bytes sent or received.

This dashboard can be filtered by source interface, domain, destination interface, and policy ID.

In order for information to appear in the *Web Sites dashboard*, web filtering must be enabled in a policy, with FortiGuard Categories enabled.

Figure 11: The *Web Sites* dashboard



Domain	Category	Browsing Time	Threat Weight	Sessions	Bytes (Sent/Received)
nytimes.com	News and Media	2h 3m 9s	0	491	143.70 M
www.bcit.ca	Unknown	12m 45s	0	84	22.90 M
nyt.com	Unknown	13m 24s	0	79	5.20 M
ubc.ca	Education	1h 17m 8s	0	65	3.71 M
moatads.com	Unknown	11m 38s	0	54	2.66 M
sfu.ca	Unknown	7m 16s	0	54	3.46 M
dynamicyield.com	Advertising	12m 1s	0	53	1.07 M
utoronto.ca	Unknown	14s	0	52	1.12 M
ubuntu.com	Reference	21s	0	44	19.59 M
google-analytics.com	Information Technology	1h 37m 38s	0	33	250.86 K
doubleclick.net	Advertising	13m 24s	0	32	467.48 K
cloudfront.net	Unknown	1h 18m 58s	0	31	1.30 M
flashtalking.com	Advertising	2m 32s	0	18	506.25 K
googlesyndication.com	Advertising	13m 24s	0	18	1.54 M
chartbeat.net	Information Technology	2m 21s	0	16	37.93 K
scorecardresearch.com	Business	13m 24s	0	16	215.78 K
krxd.net	Content Servers	10m 1s	0	15	51.83 K
revsci.net	Unknown	11m 38s	0	14	60.04 K
amazonaws.com	Unknown	18m 56s	0	12	622.93 K
fortinet.com	Information Technology	1m 8s	0	12	155.09 K
google.com	Freeware and Software Downloads	15h 26m 5s	0	11	121.19 K

Threats

The *Threats* dashboard lists the top users involved in incidents, as well as information on the top threats to your network. Additional information is provided about the threat, category, threat level, threat weight, and number of incidents.

This dashboard can be filtered by source interface, threat type, threat, destination interface, and policy ID.

In order for information to appear in the *Threats* dashboard, *Threat Weight Tracking* must be used.

Figure 12: The *Threats* dashboard

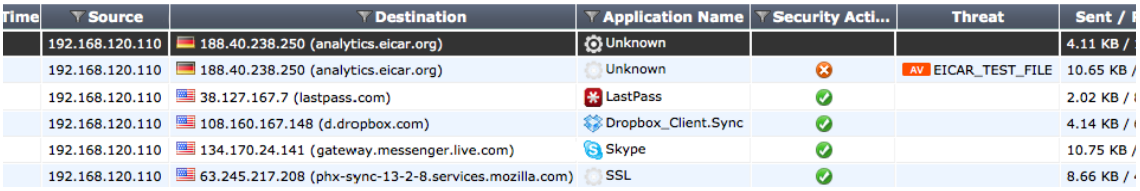
Threat	Category	Threat Le...	Threat Weight	Incidents
Failed Connection Attempts	Failed Connection Attempts	Medium	30	3

All Sessions

The *All Sessions* dashboard shows information about all FortiGate traffic. To choose which columns you wish to view, select *Column Settings* and place your desired columns in the right-hand box, in the order that you wish them to appear.

This dashboard can be filtered by source IP, destination IP, application, source device, source interface, destination interface, and policy ID. If you have set a filter in a different dashboard before viewing the *All Sessions* dashboard, that filter will remain until manually cleared.

Figure 13: The *All Sessions* dashboard



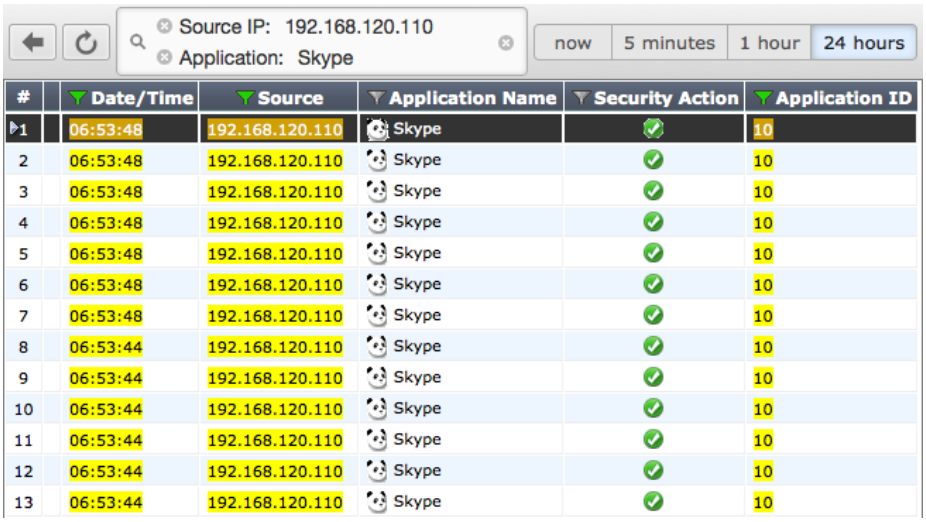
Time	Source	Destination	Application Name	Security Acti...	Threat	Sent /
	192.168.120.110	188.40.238.250 (analytics.eicar.org)	Unknown			4.11 KB /
	192.168.120.110	188.40.238.250 (analytics.eicar.org)	Unknown		AV EICAR_TEST_FILE	10.65 KB /
	192.168.120.110	38.127.167.7 (lastpass.com)	LastPass			2.02 KB /
	192.168.120.110	108.160.167.148 (d.dropbox.com)	Dropbox_Client.Sync			4.14 KB /
	192.168.120.110	134.170.24.141 (gateway.messenger.live.com)	Skype			10.75 KB /
	192.168.120.110	63.245.217.208 (phx-sync-13-2-8.services.mozilla.com)	SSL			8.66 KB /

Drilldown Options

In all FortiView dashboards except for the *All Sessions* dashboard, you can view more information about a particular session by right-clicking or double-clicking on the session to display the *Drilldown to details...* option, which opens a summary page that includes further information about applications, sources, destinations, and sessions where applicable.

From this summary page, you can access automatically filtered logs that will show a list of applicable sessions. For example, if you have picked the IP address 192.168.120.110 from the *Sources* dashboard, you can then select *Drilldown to details...* for Skype from the *Applications* column. This will open a log that displays all sessions from 192.168.1.1 that used Skype. From this page, you can select *Drilldown to details...* for any individual session, in order to view the log entry for that session.

Figure 14: Viewing Skype sessions from the Source Address 192.168.120.110



Source IP: 192.168.120.110
Application: Skype
now | 5 minutes | 1 hour | 24 hours

#	Date/Time	Source	Application Name	Security Action	Application ID
1	06:53:48	192.168.120.110	Skype		10
2	06:53:48	192.168.120.110	Skype		10
3	06:53:48	192.168.120.110	Skype		10
4	06:53:48	192.168.120.110	Skype		10
5	06:53:48	192.168.120.110	Skype		10
6	06:53:48	192.168.120.110	Skype		10
7	06:53:48	192.168.120.110	Skype		10
8	06:53:44	192.168.120.110	Skype		10
9	06:53:44	192.168.120.110	Skype		10
10	06:53:44	192.168.120.110	Skype		10
11	06:53:44	192.168.120.110	Skype		10
12	06:53:44	192.168.120.110	Skype		10
13	06:53:44	192.168.120.110	Skype		10

In the *All Sessions* dashboard, filters are also used to narrow down what results are shown. If you are viewing historical traffic in the *All Sessions* dashboard, you can also add an element to a filter by right-clicking the element and selecting *Set Filter*.

Sniffer Traffic Support

Historical traffic logging with the *FortiView* dashboards is supported for sniffer traffic.

FortiExplorer Setup Wizard Improvements

Several improvements have been made to the FortiExplorer Setup Wizard.

Removed Features

Several features have been removed from the FortiGate Setup Wizard:

- Central management configuration
- UTM: AntiSpam setup
- UTM: IPS setup
- Virtual Servers

The WAN Topology options have also been simplified so that the only option is Single Ethernet.

FortiWiFi

Several additional changes have occurred for FortiWiFi units, found in the *LAN + WiFi Settings* section of the wizard:

- The default SSID is now named `fortinetXXXX`, where XXXX is the last 4 digits of the FWF serial number.
- The default SSID is bridged with the internal network.
- The default pre-shared key is different for each FortiWiFi unit.
- A *Show Password* option has been added.

Internet Access

The following changes have been made to the *Internet Access* section of the wizard:

- Selecting *Block Viruses and Malicious Content* enables anti-virus and web filtering
- The MPAA rating system is used for *Parental Controls*

Remote VPN

In the *Remote VPN* section, an option has been added to setup dynamic DNS with FortiGuard. The option is enabled by default.

AntiVirus Inspection Mode

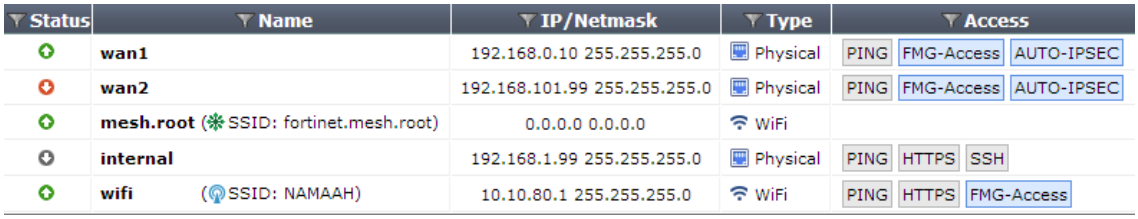
If the flow-based AntiVirus database is not enabled, the setup wizard will change the default profile to proxy-based.

Interfaces List Improvements

Several improvements have been made to the Interfaces List:

- Only interfaces with tunnels or VPNs expand to show more information.
- The Status column shows the number of clients using the interface. Clicking on the number in the status column will direct you to the *DHCP Monitor* or wireless *Client Monitor*, depending on which type of clients are using the interface.
- The protocols listed in the Access column have been assigned color codes. Secure services (HTTPS, SSH) are listed in grey, insecure services (TELNET, HTTP without HTTPS redirect enabled) are listed in red, and all other services are listed in blue.

Figure 15: The Interfaces list



Dragging Objects Between Policies in the Policy List

Objects can now be moved or copied from one policy to another in the policy list. This includes source and destination addresses, services, users, user groups, and security profiles. The default “none” object is also included.

Because of this change, a blank policy can now be created, with the configuration determined by dragging elements from other policies.

Cloning Table Objects

Table objects can now be cloned, allowing an existing object to be copied and given a new name. The object's properties can then be configured by selecting Edit.

Cloning is enabled for both Firewall Objects and Security Profiles.

DHCP-related Improvements in the Web-based Manager

A number of improvements have been made in the web-based manager, relating to DHCP:

- A DHCP Server column has been added to the interface list that shows which interfaces have been enabled as a DHCP server and the assigned IP range.
- The DHCP Client List has been improved by adding device icons and changing the Expires column to show the amount of time left on the DHCP lease.
- New addressing modes have been added to support IPv6 and PPPOE. The option for IPv6 will only appear if it has been enabled in the web-based manager, while PPPOE options only appear if IPv4 addressing is set to PPPOE as well.
- Options have been added to DHCP Monitor, allowing DCCP leases to be revoked and IP reservations to be added or edited.
- Advanced DHCP configuration can now be done through the web-based manager. To enable this feature, the following syntax must be used in the CLI:

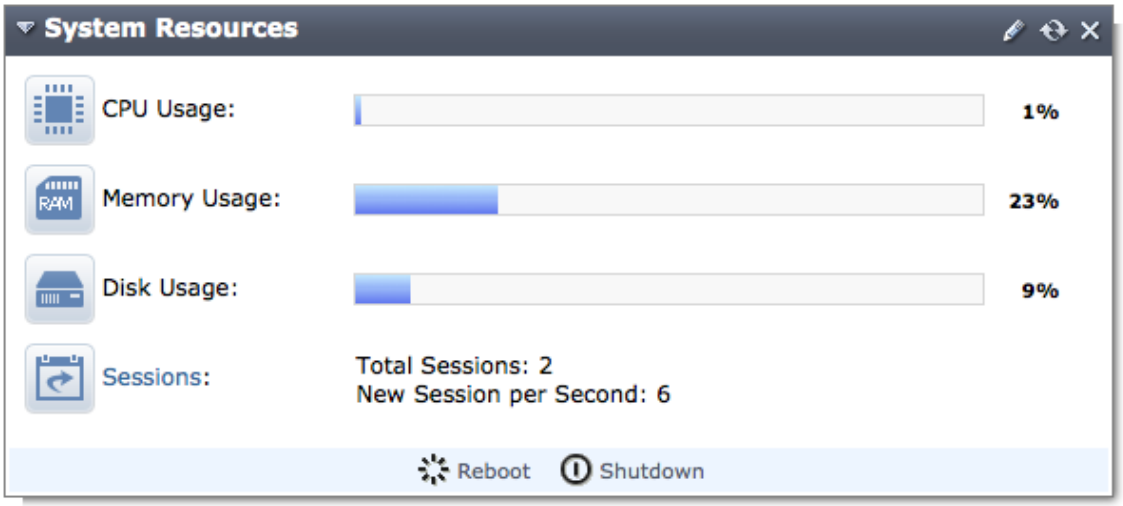
```
config system global
  set gui-dhcp-advanced enable
end
```

After this has been enabled, an *Advanced* menu can be expanded when configuring DCHP on a network interface.

System Resources Widget

The appearance of the *System Resource* widget has been changed to better illustrate the large number of CPU cores. The IPMC sensors information, about temperature, fan, and power supply unit, has also been added to the widget for some FortiGate models.

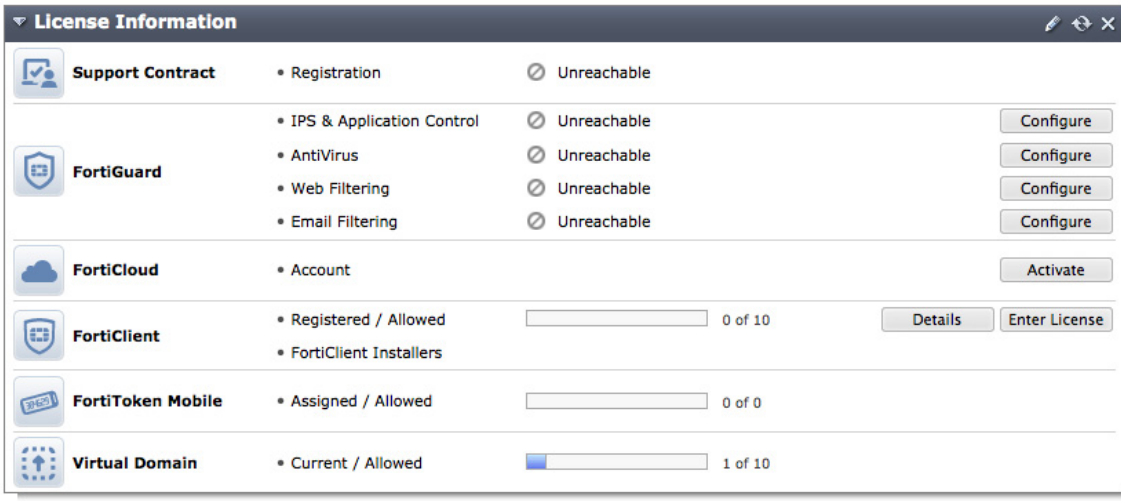
Figure 16:*System Resources* widget (on a FortiGate-100D)



License Information Widget

The appearance of the *License Information* widget has changed to clearly show the current licenses of your FortiGate. A new option has also been added to extend a license, which allows you to add a new license as soon as you buy it, rather than having to wait for the current license to expire.

Figure 17:*License Information* widget



USB Modem Widget

The following changes have occurred to the *USB Modem* widget:

- The LOC number has been removed.
- SIM State and SIM card ID fields have been added.
- MEID will be displayed if a CDMA modem is used.
- IMEI will be displayed if a GSM modem is used.

New Feature Settings Preset

A new preset, *UTM*, has been added to the Feature Settings, which are set either using the *Features* widget or by going to *System* > *Config* > *Features*. This preset turns on the following features: antivirus, web filtering, application control, and end point control. This preset is the default setting for FortiGate models 200 and below.

The preset formerly known as UTM, which turns on all features, is now called *full UTM*.

Improved Banned User List Page

The banned user list has been improved by the following changes:

- Adding a search function
- Improving sorting through column filters
- Displaying information on the event that caused the user to be quarantined

Replacement Message Improvements

The process of creating replacement message using tags and images has been simplified by the following additions:

- A right-click menu to insert tags/images
- An auto-complete feature for tags (when you begins by entering %%)
- Descriptions for each tag that appear as they are typed
- Image previews when an image tag is used
- An graphics list that allows you to select from predefined images or upload a new image
- Variables for source IP (%%SOURCE_IP%%), destination IP (%%DEST_IP%%), and user name (%%USERNAME%%) can now be added.

Sorting and Filtering Support for the Virtual IP list

In FortiOS, the virtual IP list can be sorted and filtered, allowing for easier management.

Web-based Manager Options for the FortiGate-30D

The FortiGate-30D by default views a different version of the web-based manager than other units, known as `gui-lite`. This mode can be disabled in the CLI, in order to view the standard web-based manager.

Syntax

```
config system global
   set gui-lite disable
end
```

Firewall

New firewall features include:

Menu Simplification

Security policies and firewall objects are now found in the same menu, called *Policy & Objects*.

Policies

The menu option for policies, found at *Policy & Objects* > *Policy,* has been expanded to include the following policy types:

- IPv4
- IPv6
- NAT64
- NAT46
- DoS
- IPv6 DoS
- Multicast
- Local In
- Central NAT Table
- Proxy Options
- SSL Inspection (SSL/SSH Inspection on some FortiGate models)

Objects

The following firewall objects have been grouped together under a single menu, found at *Policy & Objects* > *Objects*:

- Addresses
- Services
- Schedules
- Traffic Shapers
- Virtual IPs
- IP Pools

Other changes have been made for specific features.

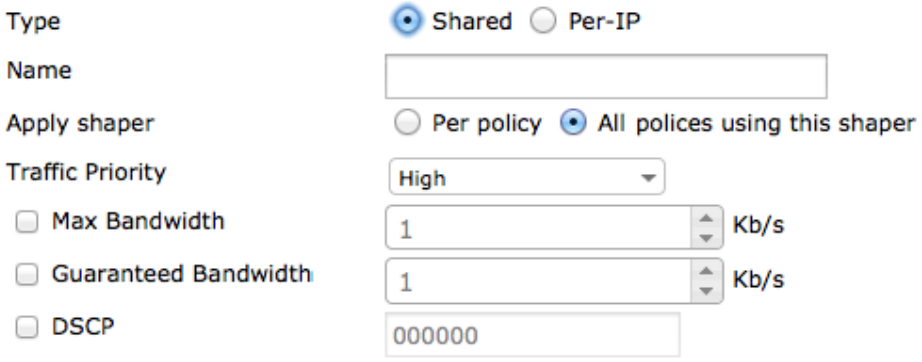
Groups

Object groups can now be made by expanding the arrow beside *Create New* and selecting *Group.*

Traffic Shapers

Shared and Per-IP shapers have been combined into a single page, with a *Type* field added to the creation page.

Figure 18: Traffic shapers creation screen

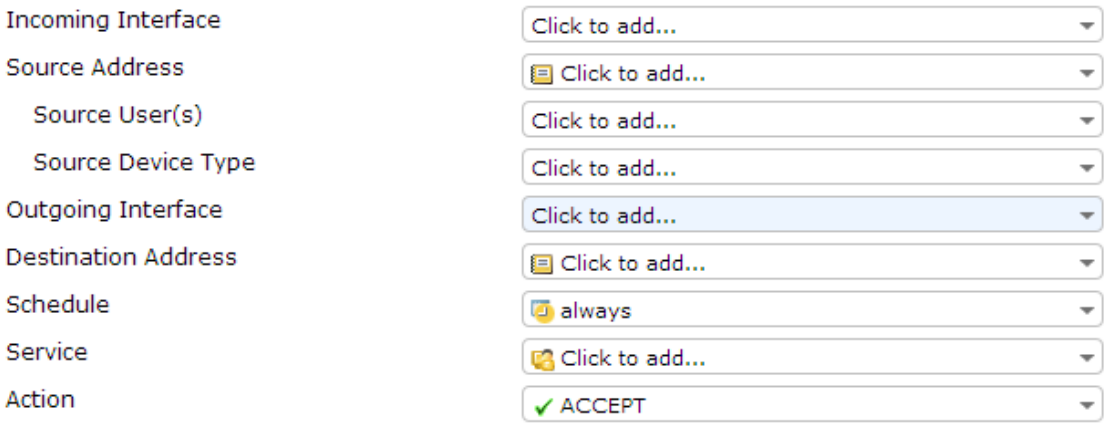


An additional column, *Type,* has also been added to the traffic shapers table.

Unified Policy Management

The different creation pages in the web-based manager for policy types and subtypes (user-identity, device identity, and VPN) have been merged into a single main policy creation page. New fields have been added for *Source User(s)* and *Source Device Type* that remove the need for multiple authentication rules in a single police. This allows for greater control and customization of policies, as a combination of these source types can be used in a single policy rather than having to pick one type.

Figure 19: The policy creation page



If both *Source User(s)* and *Source Device Type* are set, then traffic must match both fields in order to be accepted by the policy. Both these fields are optional; only *Source Address* must be set.

For policies that require user or device authentication, there is an implicit fall-through to allow traffic to be checked against other policies if it does not match the authentication requirements. This option cannot be disabled and the CLI command `set fall-through-unauthenticated` has been removed.

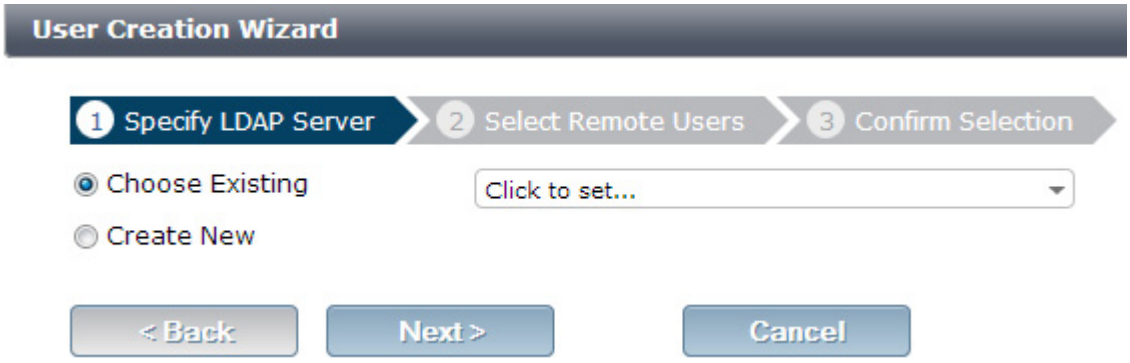
For more information about security policies in FortiOS 5.2, please see the FortiGate Cookbook recipe *Creating and ordering security policies to provide access to different users and devices*, found at docs.fortinet.com.

To create a policy for SSL VPNs, an SSL VPN interface is created and used as the source interface. For more information about this interface creation, see “SSL VPN Configuration” on page 86.

Importing LDAP Users for a Security Policy

The LDAP user importing wizard can now be launched during the creation of a new security policy, by selecting *Import LDAP users* in the dropdown menu when you are adding users to the policy.

Figure 20: The LDAP user importing wizard



Dynamic VIP According to DNS Translation

Dynamic virtual IPs according to DNS translation can now be configured.

When a dynamic virtual IP is used in a policy, the dynamic DNS translation table is installed along with the dynamic NAT translation table into the kernel. All matched DNS responses will be translated and recorded regardless if they hit the policy. When a client request hits the policy, dynamic NAT translation will occur if it matches a record, otherwise the traffic will be blocked.

Syntax

```
config firewall vip
  edit 1
    set type dns-translation
    set extip 192.168.0.1-192.168.0.100
    set extintf dmz
    set dns-mapping-ttl 604800
    set mappedip 3.3.3.0/24 4.0.0.0/24
  end
end
```

GTP Rate Limiting

New methods of GPRS Tunneling Protocol (GTP) rate limiting are available in FortiOS 5.2.

Per-Stream Rate Limiting

FortiOS 5.2 supports per-stream rate limiting of GTP and the ability to apply rate limiting separately for GTPv0 and GTPv1, as well as for GTPv2.

This feature required the addition of the following CLI commands: `message-rate-limit-v0`, `message-rate-limit-v1`, and `message-rate-limit-v2`. The commands `message-rate-limit-v0` and `message-rate-limit-v1` are only visible when `rate-limit-mode` is set to `per-stream`, while message-rate-limit is visible when rate-limit-mode is set to `per-profile`. The command `message-rate-limit-v2` is always visible, since GTPv2 message numbering and naming are different from GTPv0/v1.

The following features have also been added:

- Warning limit support.
- Per-version message rate limiting.
- A log for rate limiting warning called `rate-limited-warning`.

In addition, FortiOS Carrier now indicates the GTP version in rate limiting log messages and writes a rate limiting warning log message when a packet exceeds the rate limiting threshold.

Syntax

```
config firewall gtp
   edit <name>
      set rate-limit-mode {per-profile | per-stream}
      set warning-threshold {0-99}
      config {message-rate-limit-v0 | message-rate-limit-v1 |
           message-rate-limit-v2}
         set create-pdp-request <rate-limit>
         set delete-pdp-request <rate-limit>
         set echo-request <rate-limit>
      end
   end
end
```

Per-APN Rate Limiting Profiles

In FortiOS 5.2, GTP rate limiting profiles can be based per-APN, as well as per-IP. To use this feature, the rate limit for each specific APN needs to be configured in the CLI, as there is no default rate limit.

Syntax

```
config firewall gtp profile
   set rate-limit-mode per-apn
   config per-apn-shaper
      edit <ID>
         set apn <string>
         set version <version>
         set rate-limit <rate-limit>
      end
   end
end
```

Object UUID Support

UUID is only supported on large-partition platforms (>=128M).

A Universally Unique Identified (UUID) attribute has been added to some firewall objects, including virtual IPs and virtual IP groups for IPv4, IPv6, NAT46, and NAT64, so that the logs can record these UUID to be used by a FortiManager or FortiAnalyzer unit.

The UUID of an object can either be generated automatically or assigned through the CLI. To view the UUID for these objects in a FortiGate unit's logs, `log-uuid` must be set to `extended mode`, rather than `policy-only`, which only shows the policy UUID in a traffic log.

Syntax

```
config sys global
  set log-uuid {disable | policy-only | extended}
end

config firewall {policy | policy6 | policy46 | policy64 | address|
     addres6 | addgrp | addgrp6}
  edit <1>
    set uuid <8289ef80-f879-51e2-20dd-fa62c5c51f44>
  end
end
```

Configuring the Class of Service Bit

FortiGate units can now configure the value of the Class of Service (CoS) bit, also called Priority Code Point (PCP).

The value of CoS in forward direction (fwd) and reverse direction (rev) is set in the policy/policy6 table using the CLI. The value can be set either as 255, to allow passthrough, or given a priority between 0 and 7.

Syntax

```
config firewall {policy | policy6}
  set vlan-cos-fwd <int>
  set vlan-cos-rev <int>
end
```

Hairpinning for NAT64 and NAT46

In FortiOS 5.2, NAT64 and NAT46 support hairpinning between hosts that are located in the same network behind a single external IP address. Hairpinning allows endpoints on the internal network to communicate using external IP addresses and ports.

In order to allow hairpinning, `set permit-any-host` must be enabled in the NAT64 or NAT46 firewall policy.

Maximum Number of Available Virtual IPs Increased

The maximum limit of available virtual IPs has been increased on 1U FortiGate models (FortiGate-100 to 800 series) to 16,000 and on 2U FortiGate models (FortiGate-1000 to 3810 series) to 32,000.

Security Profiles

New security profiles features include:

- Menu and Options Simplification
- SSL Inspection
- Web Filtering
- Application Control
- Flow-based Antivirus
- Intrusion Protection System (IPS)
- Vulnerability Scanning Visibility
- Client Reputation

Menu and Options Simplification

The menus and options for security profiles have changed in several ways. The basic profile/sensor/settings options have been left in the menu for each feature, while extra tables are now located in the *Advanced* menu. Other changes have been made for specific features.

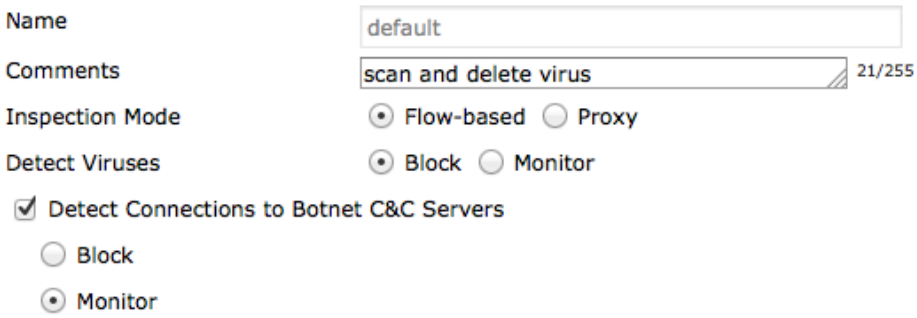
AntiVirus

Several changes have been made for the configuration options in AntiVirus profiles, as visible options change depending on whether *Inspection Mode* is set to *Flow-based* or *Proxy*.

Flow-based Profile Options

If flow-based inspection is used for AntiVirus, the only additional options that can be configured in the web-based manager are for what actions will be taken for detected viruses and connections to Botnet C&C servers. *Detect Viruses* can be set to either *Block* or *Monitor.* These same two options are available for Botnet C&C servers, if detection is enabled.

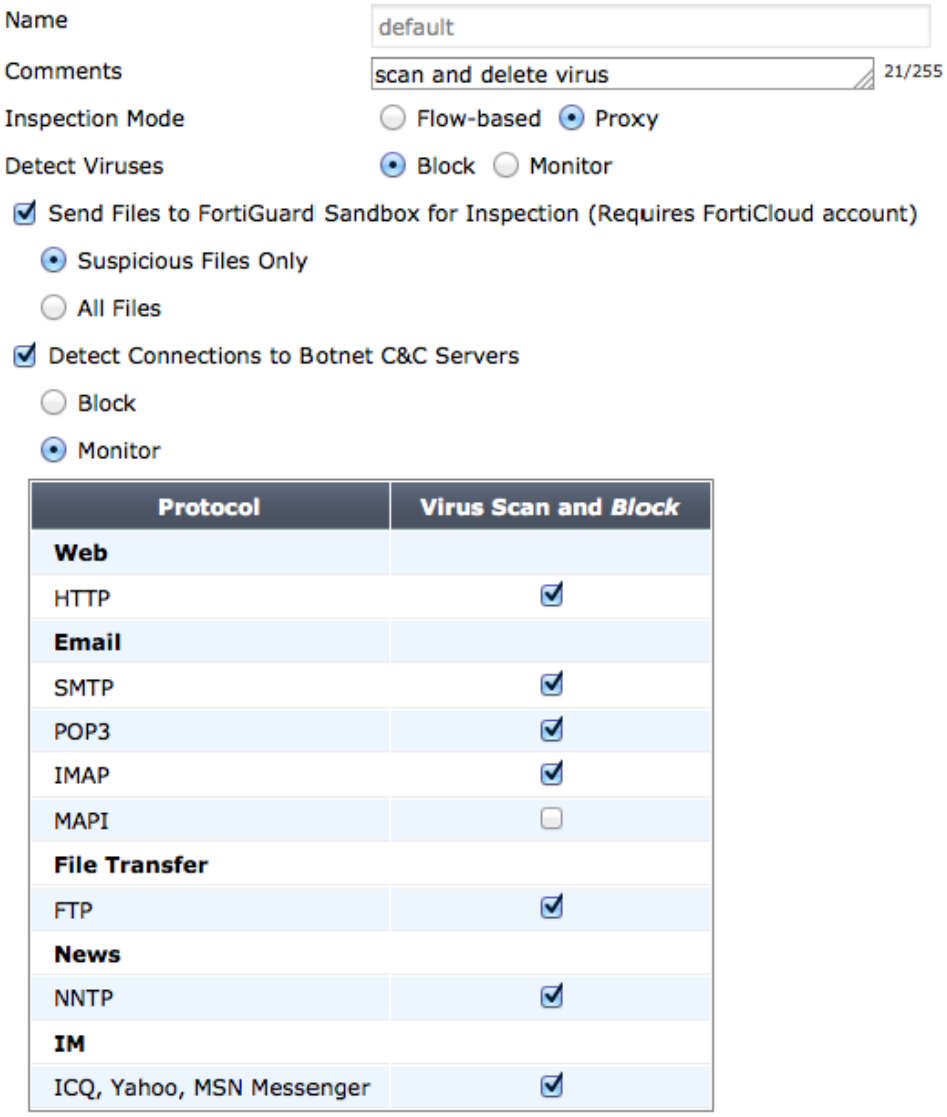
Figure 21: Flow-based options for AntiVirus



Proxy Options

If proxy inspection is used for AntiVirus, the addition *Block* or *Monitor* options are available for both detected viruses and Botnet C&C servers. The previous options for using FortiSandbox and protocol selection are also available.

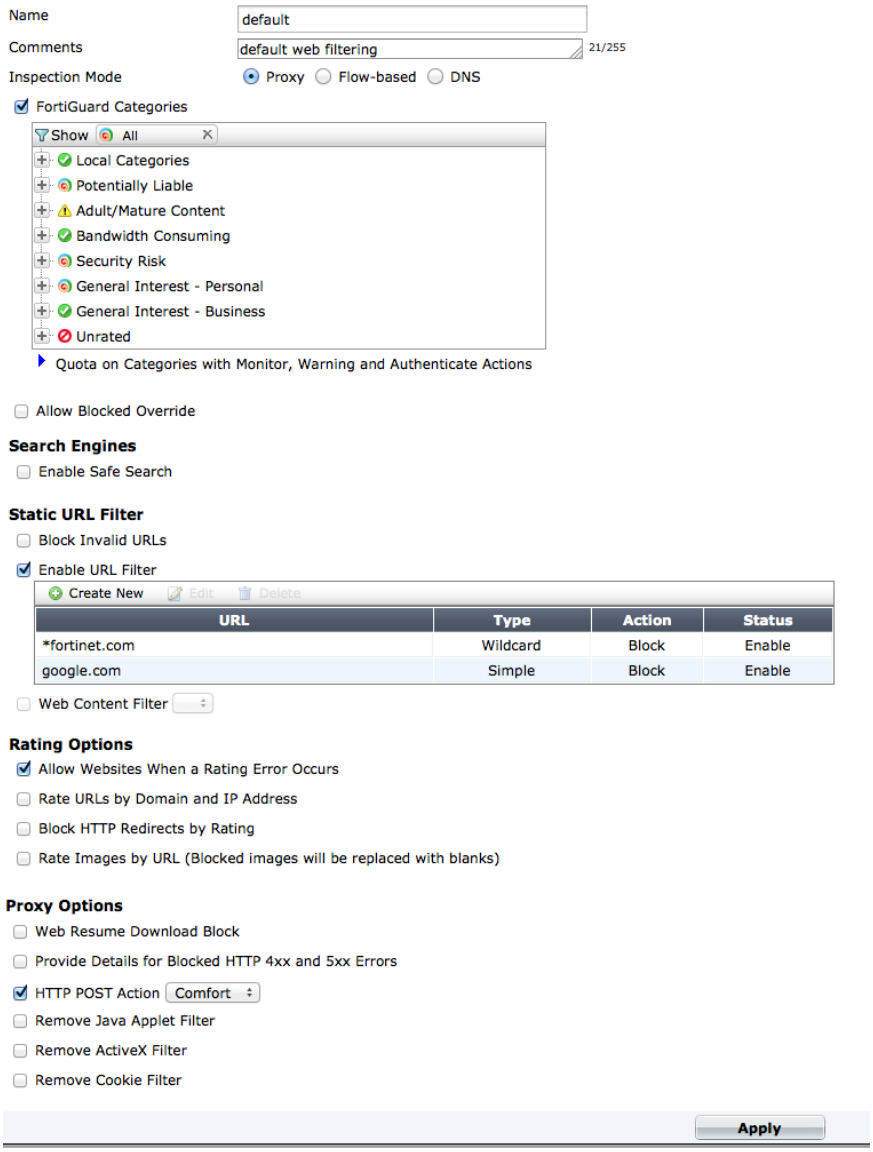
Figure 22: Proxy options for AntiVirus



Web Filter

The web filter profile page has been expanded to contain settings for *FortiGuard Categories*, *Search Engines*, *URL Filters*, *Ratings Options*, and *Proxy Options*.

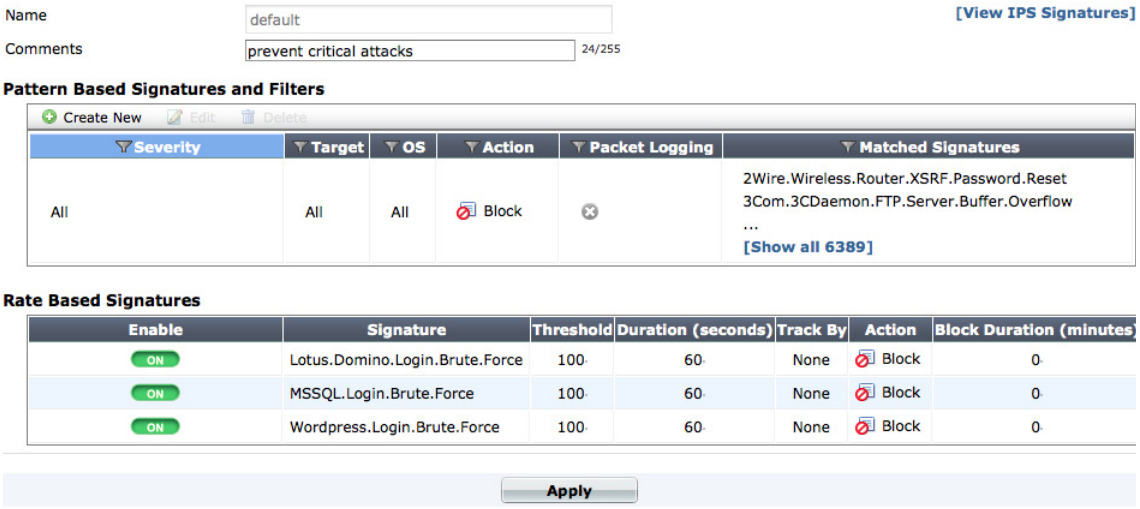
Figure 23: The web filter profile page



Intrusion Protection

The IPS sensor page now contains options for *Pattern Based Signatures and Filters* and *Rate Based Signatures*. The full list of IPS Signatures can be accessed from the sensor page by selecting *View IPS Signatures*.

Figure 24: The IPS sensor page

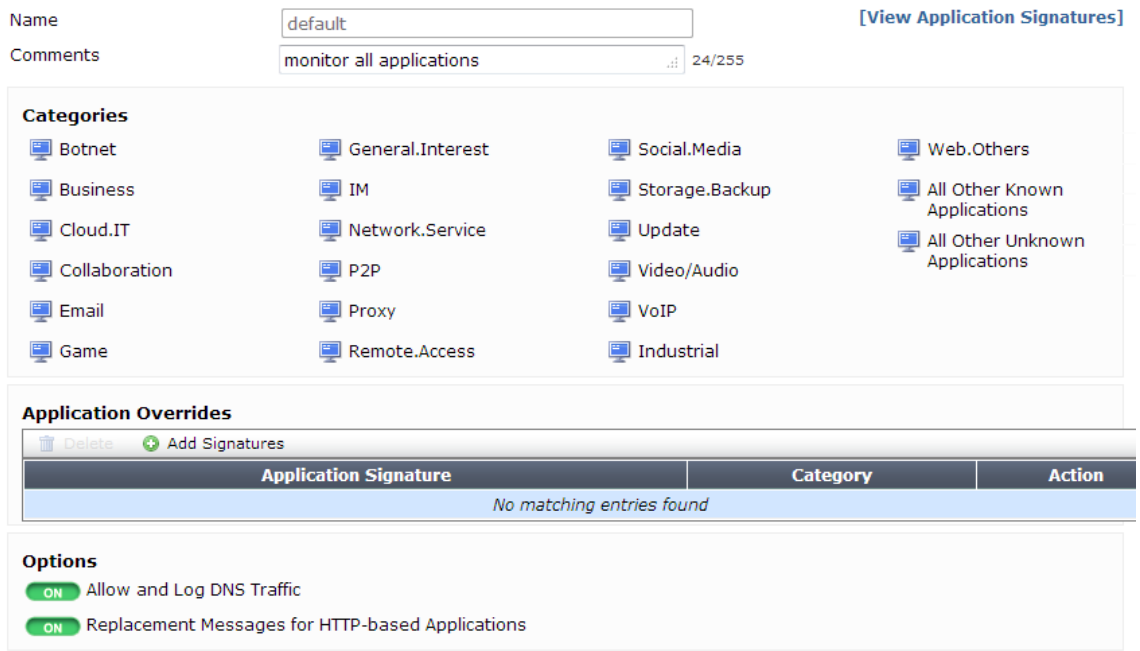


Application Control

The following changes have been made to improve usability in the web-based manager:

- A new category list has been made that appears on the sensor page, found by going to *Security Profiles* > *Application Control*. When you click on a category, a drop down menu appears, allowing the action for that category to be changed. You can also select to view all the application control signatures for that category.
- Application signatures can be viewed by selecting *View Application Signatures*.
- *Application Overrides* allow you to change the action taken for specific signatures/applications.
- The application filter sorting criteria popularity, technology, and risk have been removed.

Figure 25: The application control sensor page



Advanced Options

A new advanced menu has been added that contains the following features:

- Web rating overrides
- Web profile overrides
- DLP fingerprinting

Web Rating Overrides can also now be used to edit or delete custom website categories.

SSL Inspection

There have been several changes to how SSL Inspection is handled on a FortiGate unit.

Automatic Inspection When Security Profiles are Used

If any security profile is used in a security policy, SSL inspection will automatically be enabled, at which point an SSL mode must be selected (see below for more details).

HTTPS Scanning Without Deep Inspection

The following changes have been made in order to allow HTTPS traffic to be scanned without enabling deep inspection:

- There are now two modes for SSL inspection: certificate inspection (`certificate-inspection` in the CLI), which only inspects the SSL handshake, and `deep inspection (deep-inspection` in the CLI), which enables full deep inspection of SSL traffic (this was previously the default mode for SSL inspection).
- The CLI command `https-url-scan` has been removed.
- `deep-inspection-options` has been renamed `ssl-ssh-profile`.
- The SSL `inspect-all` option and the `https status` option now have three states: `disable`, `certificate-inspection`, and `deep-inspection`. The status option for the other protocols now use `deep-inspection` instead of `enabled`.

When a new policy or profile group is created, the SSL inspection profile `certificate-inspection` is automatically added.

SSL/Deep Inspection Exemptions

The options for configuring exemptions to SSL/Deep Inspection is now configured as part of the deep inspection options, rather than FortiGuard web filtering. Exemptions can be added to SSL inspection by going to *Policy & Objects* > *Policy* > *SSL Inspection* or through the CLI.

Certain applications, such as iTunes and Dropbox, require a specific certificate to be used, rather than using the use the system's certifciate store. Because of this, the default deep

inspection profile, `deep-inspection`, has exemptions configured for these applications by default in FortiOS 5.2.

Syntax

```
config firewall ssl-ssh-profile
  edit <name>
    config ssl-exempt
      edit <id>
        set type {fortiguard-category | address | address6}
        set category <id>
        set address <string>
      end
    end
  end
end
```

Generating Unique CA and Server Certificates

A FortiGate unit will now generate default SSL inspection CA and server certificates that are unique to that unit the first time the certificates are required. Previously, FortiGate units all have the same default CA and server certificates.

There are some exceptions: for example, in a HA cluster all FortiGate units need the same CA and server certificates. The certificates can also be changed as required for load balancing and other configurations.

Existing customers will not be affected by this change, as FortiOS 5.2 will not change the current defaults on upgrade.

You can use the CLI commands below to generate new certificates that will be unique to your FortiGate unit.

The following command re-generates the default SSL inspection CA certificate:

```
execute vpn certificate local generate default-ssl-ca
```

The following command re-generates the default SSL inspection server certificate:

```
execute vpn certificate local generate default-ssl-serv-key
```

Server Certificates

In FortiOS 5.2, two methods are available to support server certificates and allow inbound traffic to be inspected: *Multiple Clients Connecting to Multiple Servers* (`re-sign` in the CLI) or *Protecting SSL Server* (`replace` in the CLI).

The default setting for SSL Inspection is *Multiple Clients Connecting to Multiple Servers.*This setting can be changed by going to *Policy & Objects* > *Policy* > *SSL Inspection* or through the CLI.

Syntax

- Uploading a new server certificate:

```
config firewall ssl-ssh-profile
  edit <name>
    set server-cert-mode replace
    set server-cert <certificate>
  end
end
```

- Re-signing the server certificate:

```
config firewall ssl-ssh-profile
  edit <name>
    set server-cert-mode re-sign
    set caname <name>
    set certname <name>
  end
end
```

Web Filtering

There have been several changes made to web filtering in FortiOS 5.2.

HTTPS for Warnings and Authentication

HTTPS protocol can now be used when sending web filtering warnings or requiring a user to authenticate, including authentication for web filter overrides.

Syntax

```
config webfilter fortiguard
  set ovrd-auth-https enable
  set warn-auth-https enable
end
```

Modifying HTTP Request Headers

In FortiOS 5.2, you can add, modify, and remove header fields in HTTP request when scanning web traffic in proxy-mode. If a header field exists when your FortiGate receives the request, its content will be modified based on the configurations in the URL filter.

Syntax

```
config web-proxy profile
  edit <name>
    config headers
      edit <ID>
        set name <name>
        set content <string>
      end
    end
  end
end
```

Restrict Google Access to Corporate Accounts

A new option has to web filtering to restrict Google access to specific domains. This allows you to block access to some Google accounts and services while allowing access to corporate Google accounts.

To use this option, go to *Security Profiles* > *Web Filter* and select *Restrict Google Account Usage to Specific Domains* under *Proxy Options*. You can then add the appropriate Google domains that will be allowed.

After the web filter profile has been created, this feature is applied differently in the case of transparent proxy vs. explicit proxy. For transparent proxy, the web filter profile is added to a security policy. For explicit proxy, the web filter profile must be added to an explicit proxy profile.

This feature can also be configured using the CLI, where use of the Modifying HTTP Request Headers feature (see above) is required. In the following example, access to Personal Gmail accounts is blocked while access to Google Business Mail is allowed.

Syntax

1. The web-proxy profile is configured to with a modified header:

```
config web-proxy profile
  edit "restrict-google-accounts-1"
    config headers
      edit 1
        set name "X-GoogApps-Allowed-Domains"
        set content "example.com"
      end
    end
  end
```

2. A URL filter is configured to use the web-proxy profile:

```
config webfilter urlfilter
  edit 1
    set name "GMAIL_TEST"
    config entries
      edit 1
        set url "*.google.com"
        set type wildcard
        set action allow
        set web-proxy-profile "restrict-google-accounts-1"
      end
    end
  end
```

3. A webfilter profile is configured that uses the URL filter:

```
config webfilter profile
  edit "GMAIL_TEST"
    ......
    config web
      set urlfilter-table 1
    end
    config ftgd-wf
      ......
    end
  end
end
```

4. **Transparent proxy -** the webfilter profile is applied to a security policy:

```
config firewall policy
  edit 1
    set srcintf "LAN"
    set dstintf "WAN"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set webfilter-profile "GMAIL_TEST"
    set profile-protocol-options "default"
    set ssl-ssh-profile "deep-inspection"
    set nat enable
  end
end
```

5. **Explicit proxy -** the web-proxy policy and the web filer profile are applied to an explicit proxy policy:

```
config firewall explicit-proxy-policy
  edit 1
    set proxy web
    set dstintf "WAN"
    set srcaddr "all"
    set dstaddr "all"
    set service "webproxy"
    set action accept
    set schedule "always"
    set webproxy-profile "restrict-google-accounts-1"
    set utm-status enable
    set webfilter-profile "GMAIL_TEST"
    set profile-protocol-options "default"
    set ssl-ssh-profile "deep-inspection"
  end
end
```

Referer Added to URL Filtering

You can now add a referer to URL filters. If a referer is specified, the host name in the referer field of the HTTP require will be compared for any entry that contains the matching URL. If the referer matches, then the specified action will be performed by proxy.

The referer can also be set in the web-based manager, but only if advanced web filter features has been enabled using the following command:

```
config system global
  set gui-webfilter-advanced enable
end
```

After this command is used, a new column will be created in *Security Profiles* > *Web Filter* > *Static URL Filter* to set the referer.

The command `set referrer-host` has been added to the CLI. The CLI has also changed so that URL filters are now identified by their IDs, and the URL values can be set under each entry.

Syntax

```
config webfilter urlfilter
  edit <ID>
    config entries
      edit 1
        set url <url>
        set referrer-host <url>
        set type {simple | regex | wildcard}
        set action {block | allow | monitor | exempt}
        set status {enable | disable}
      end
    end
  end
end
```

FortiGuard Rating Checks for Images, JavaScript, CSS, and CRL

Web filter profiles that use FortiGuard rating checks can now be configured to rate images, JavaScript, CSS, and CRL.

Syntax

```
config webfilter profile
  edit <name>
    config ftgd-wf
      set rate-javascript-urls enable
      set rate-css-urls enable
      set rate-crl-urls enable
      set rate-image-urls enable
    end
  end
end
```

Additional Replacement Message Variables

Along with the variables for source IP (%%SOURCE_IP%%), destination IP (%%DEST_IP%%), and user name (%%USERNAME%%) that have been added for all replacement messages, the following variables can now be added to replacement messages for web filtering:

- Group name (%%GROUPNAME%%)
- Policy UUID (%%POLICY_UUID%%)
- FortiGate Hostname (%%FGT_HOSTNAME%%)

New Daemon for Overrides and Warnings

The new daemon `ovrd` is used in FortiOS 5.2 to handle user-level webfilter overrides and warnings.

Application Control

There have been several changes made to application control.

Deep Inspection for Cloud Applications

Deep inspection allows the following information to be examined and logged for cloud applications:

- Information about user logins and file transfers for cloud applications.
- Video names will be shown in the *Application Details* column for video streaming applications such as Youtube and Vimeo.
- The following new fields have been added to both the application control log and to traffic logs: cloud user, cloud action, file name, and file size.

To enable this feature, turn on *Deep Inspection of Cloud Applications* in an application control profile. It can also be enabled using the CLI.

Syntax

```
config application list
  edit <name>
    set deep-app-inspection enable
  end
end
```

Using the CLI, you can specify a global timeout for the deep application control database. Any database entries that exceed the timeout will be deleted. A global size threshold on the number of entries in the deep application control database can also be set.

When the total number of entries exceeds this threshold, the internal timeout value will be reduced to accelerate entry retiring. Both values are set to 0 (unlimited) by default.

Syntax

```
config ips global
  set deep-app-insp-timeout <integer>
  set deep-app-insp-db-limit <integer>
end
```

A new option, `--deep_ctrl`, has also been added to the syntax for IPS/application control signatures.

Several new CLI commands have also been added for diagnose and debugging:

- `diagnose ips dac info`
- `diagnose ips dac clear`
- `diagnose ips debug enable dac`

Traffic Shaping Settings

Traffic shaping settings can be applied to categories of applications that are part of the application control sensor.

To apply settings, select a category and set it to *Traffic Shaping.* The *Traffic Shaping Settings* options will appear, allowing you to select the settings for forward and reverse traffic shaping. These settings will be applied to all categories set to *Traffic Shaping* in your application control sensor.

5-Point-Risk Rating

A new rating system will be used for all pages related to application control, including the application list, the application filters list, traffic logs, the *FortiView Applications* dashboard, and the *FortiView All Sessions* dashboard. Risk levels are indicated in the various tables and logs by using a series of icons.

The rating system is as follows:

Icon	Risk Level	Description	Example
	Critical	Applications that are used to conceal activity to evade detection	Tor, SpyBoss
	High	Applications that can cause data leakage, or prone to vulnerabilities or downloading malware	Remote Desktop, File Sharing, P2P
	Medium	Applications that can be misused	VoiP, Instant Messaging, File Storage, WebEx, Gmail
	Elevated	Applications are used for personal communications or can lower productivity	Gaming, Facebook, Youtube
	Low	Business Related Applications or other harmless applications	Windows Updates

Replacement Message

A replacement message has been added that will appear when an application has been blocked.

This replacement message can be enabled in the CLI.

Syntax

```
config application list
  edit <name>
    set app-replacemsg {enable | disable}
  end
end
```

Support for SPDY Protocol

The SPDY protocol, and its required SSL/TLS component, is now recognized within application control profiles. It is counted as part of application traffic for Google and other sources that use the protocol.

Support for Non-HTTP WAN Optimization and Explicit Proxy Traffic

Application control is now supported for both non-HTTP WAN optimization traffic and explicit proxy traffic.

Flow-based Antivirus

In FortiOS 5.2, flow-based AntiVirus has been improved to have the same enhanced performance as flow-based antivirus scanning in FortiOS 5.0 while providing the same accuracy and many of the extended features of proxy-based antivirus.

Flow-based AntiVirus now allows data to accumulate until it detect the end of a file. When the end is reached, traffic is paused and data is sent asynchronously for analysis. When the results are received, the traffic is either allowed to resume or the connection is reset.

Because of this change, the default AntiVirus profile on a FortiGate uses flow-based inspection. Flow-based inspection can also utilize the extended AntiVirus database. Detecting and reporting only occurs when AntiVirus is enabled in the security policy.

Flow-based AntiVirus is also supported for sniffer policies.

Intrusion Protection System (IPS)

There have been several changes made to intrusion protection system (IPS).

Adjusting Rate Based Signatures

Setting for rate based IPS signatures can now be edited in the web-based manager as part of an IPS sensor. In each sensor, you can enable a selected list of rate based signatures and adjust threshold, duration, track by setting, action, and block duration.

Figure 26: Rate Based Signatures list

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
ON	Lotus.Domino.Login.Brute.Force	100	60	None	Block	0
ON	MSSQL.Login.Brute.Force	100	60	None	Block	0
ON	Wordpress.Login.Brute.Force	100	60	None	Block	0

Extensible Meta Data

Extensible meta data allow you to specify custom options in IPS signatures that are delivered to your FortiGate without interpretation, in order to make signatures easier to find and understand for the FortiGate administrator. Four types of meta data options are supported: integers, bitmaps, enumerables, and strings.

Example

In this example, a set of meta data is declared and then used to create IPS signatures.

1. The meta data is declared:

```
F-META2( --name points; --index 12; --type integer; )
F-META2( --name flags; --index 34; --type bitmap; --value foo:1;
     --value bar:2; --value baz:4; )
F-META2( --name dr_seuss; --index 56; --type enum; --value "One
     Fish":1; --value "Two Fish":2; --value "Red Fish":3; --value "Blue
     Fish":4; )
F-META2( --name secret; --index 78; --type string; )
```

2. The meta data is used:

```
F-SBID( --points 42; ... )
F-SBID( --flags foo; --flags baz; ... )
F-SBID( --dr_seuss "One Fish"; ... )
F-SBID( --secret "Abracadabra"; ... )
```

Extended Database

In FortiOS 5.2, the IPS extended database is enabled by default for all FortiGate models that have multiple CP8.

Support for Non-HTTP WAN Optimization and Explicit Proxy Traffic

IPS is now supported for both non-HTTP WAN optimization traffic and explicit proxy traffic.

Vulnerability Scanning Visibility

The options to configure vulnerability scanning either in the web-based manager or the CLI are also only available in NAT/Route mode.

Vulnerability scanning options in the web-based manager are now hidden by default. To enable vulnerability scanning, go to *System* > *Config* > *Features*, select *Show More*, turn on *Vulnerability Scan*, and select *Apply*.

Vulnerability scanning is also hidden by default for FortiClient profiles until being enabled in the CLI. To enable scanning, enter the following commands:

```
config endpoint-control profile
  edit <profile-name>
    config forticlient-winmac-settings
      set forticlient-vuln-scan {enable | disable}
      set forticlient-vuln-scan-schedule {daily | weekly | monthly}
      set forticlient-vuln-scan-on-registration {enable | disable}
      set forticlient-ui-options {av | wf | af | vpn | vs}
    end
  end
end
```

Removed IM Proxy Options from the CLI

The proxy options related to instant messaging (IM) functions and attributes have been removed from the CLI in FortiOS 5.2. This includes the following commands:

- `config imp2p`
- `get imp2p`
- The DLP sensor options for AIM, ICQ, MSN, and Yahoo protocols.
- The AntiVirus profile option `config im`.
- The AntiVirus quarantine options for IM.
- The Application Control profile options for IM.
- The firewall profile protocol options for IM.

Client Reputation

The 5.0 feature client reputation has been renamed Threat Weight in FortiOS 5.2 and has been moved from Security Profiles to *Log & Report* > *Log Config* > *Threat Weight*. It can now be configured in the CLI using the command `config log threat-weight`.

IPsec VPN

New IPsec VPN features include:

- VPN Creation Wizard
- Internet Key Exchange (IKE)
- Dynamic IPsec Route Control
- Default Lifetimes and Proposal Values
- Prioritizing DH Group Configuration
- IPv6 Support for IPsec Phase 2
- IPsec VPN Support with the FortiController-5103B

VPN Creation Wizard

Several improvements have been made to the *VPN Creation Wizard.*

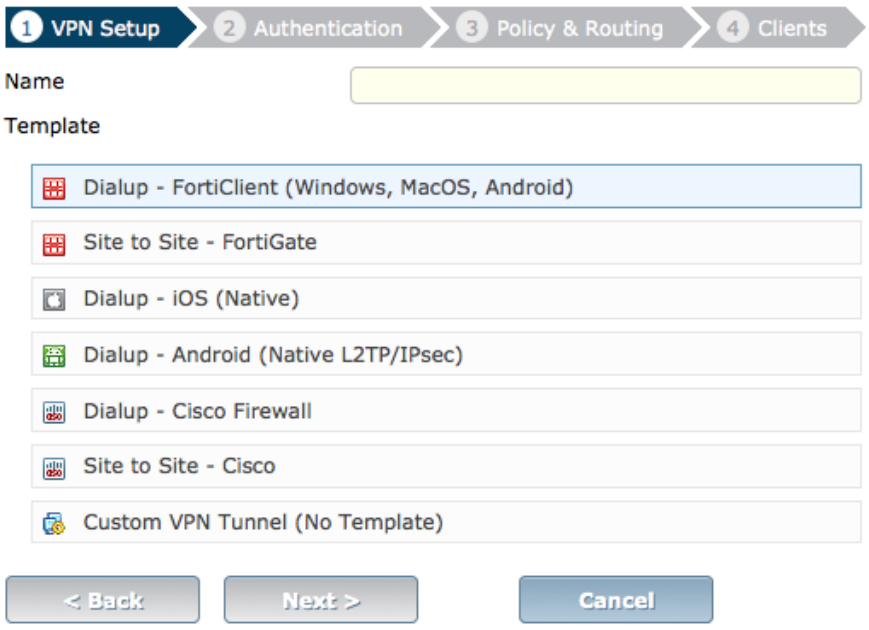
New Menu

The Wizard can now be found by going to *VPN* > *IPsec* > *Wizard.*

Expanded VPN Options

The number of VPN options available in the Wizard has increased to allows you to easily create VPN tunnels for a greater variety of scenarios.

Figure 27: Expanded VPN Options for the VPN Creation Wizard



For more information about using the VPN Wizard, see The FortiGate Cookbook recipe *Configuring an IPsec VPN for iOS devices*, found at docs.fortinet.com.

Tunnel Templates

Several tunnel templates have been added to the Wizard that cover a variety of different types of IPsec VPNs. A list of these templates appears on the first page of the Wizard, which is found by going to *VPN* > *IPsec* > *Tunnels*.

To view more information about a template, highlight the template and select *View.*

Figure 28: Tunnel Templates list

Template	Description
Dialup - FortiClient (Windows, MacOS, Android)	On-demand tunnel for users using the FortiClient software.
Site to Site - FortiGate	Static tunnel between this FortiGate and a remote FortiGate.
Dialup - iOS (Native)	On-demand tunnel for iPhone/iPad users using the native iOS IPsec client.
Dialup - Android (Native L2TP/IPsec)	On-demand tunnel for Android users using the native L2TP/IPsec client.
Dialup - Cisco Firewall	On-demand tunnel for users using the Cisco IPsec client.
Site to Site - Cisco	Static tunnel between this FortiGate and a remote Cisco firewall.

Internet Key Exchange (IKE)

There have been several changes in FortiOS 5.2 made concerning Internet Key Exchange (IKE) protocol.

Multiple Interfaces

An IPsec policy can now contain multiple source and destination interfaces. This feature is supported for combinations of IPsec interfaces, physical interfaces, and zones (including those with a combination of physical and IPsec interfaces).

It is not supported for SSL VPN interfaces.

Mode-Configuration

When IKE Mode-Configuration is enabled, multiple server IPs can be defined in IPsec Phase 1. This mode also allows IP information to be sent the client if attribute 28681 is requested.

Mode-Configuration is configured through the CLI. An example of a complete configuration is shown below:

```
config vpn ipsec phase1-interface
  edit "vpn-p1"
    set type dynamic
    set interface "wan1"
    set xauthtype auto
    set mode aggressive
    set mode-cfg enable
    set proposal 3des-sha1 aes128-sha1
    set dpd disable
    set dhgrp 2
    set xauthexpire on-rekey
    set authusrgrp "FG-Group1"
    set ipv4-start-ip 10.10.10.10
    set ipv4-end-ip 10.10.10.20
    set ipv4-dns-server1 1.1.1.1
    set ipv4-dns-server2 2.2.2.2
    set ipv4-dns-server3 3.3.3.3
    set ipv4-wins-server1 4.4.4.4
    set ipv4-wins-server2 5.5.5.5
    set domain "fgt1c-domain"
    set banner "fgt111C-banner"
    set backup-gateway "100.100.100.1" "100.100.100.2" "host1.com"
        "host2"
  end
end
```

Certificates Groups

IKE certificate groups consisting of up to four RSA certificates can now be used in IKE phase 1. Since CA and local certificates are global, the IKE daemon loads them once for all VDOMss and indexes them into trees based on subject and public key hash (for CA certificates), or certificate name (for local certificates). Certificates are linked together based on the issuer, and certificate chains are built by traversing these links. This reduces the need to keep multiple copies of certificates that could exist in multiple chains.

IKE certificate groups can be configured through the CLI.

Configuring the IKE local ID

```
config vpn certificate local
  edit <name>
    set ike-localid <string>
    set ike-localid-type {asn1dn | fqdn}
  end
end
```

Adding certificates to the group

```
config vpn ipsec {phase1 | phase1-interface}
   edit <name>
      set rsa-certificate <name>
   end
end
```

Authentication Methods

Three new authentication methods have been implemented for IKE: ECDSA-256, ECDSA-384, ECDSA-521.

In order to support these three methods, the following changes have been made to the CLI:

1. `rsa-signature` has been renamed to `signature` for both policy-based and interface-based IPsec VPN.
2. `rsa-certificate` has been renamed to `certificate` for both policy-based and interface-based IPsec VPN.

Inheriting Groups from the Security Policy

IPsec VPNs can now be configured to authenticate users again the group(s) specified in a policy that refers to the VPN's phase 1. To use this feature, do the following:

1. Go to *VPN* > *IPsec* > *Tunnels* and edit a tunnel.
2. Set *XAUTH Type* to *Auto Server*.
3. Set *User Group* to *Inherit Groups from Policy*.

This feature can be used for both interface-based and policy-based IPsec VPN phase 1s.

Syntax

```
config vpn ipsec {phase1 | phase1-interface}
   edit <name>
      set xauthtype auto
   end
end
```

Assigning Client IP Addresses Using the DHCP Proxy

IKE can now use the system DHCP proxy to assign client IP addresses.

To use this feature, the DHCP proxy must be enabled and a IP set. Up to 8 addresses can be selected for either IPv4 or IPv6. After the DHCP proxy has been configured, the `assign-up-from` command is used to select assign IP address via DHCP.

Syntax

1. Enabling the DHCP proxy and setting an IP range.

```
config system settings
   set dhcp-proxy enable
   set dhcp-server-ip <IP_address>
   set dhcp6-server-ip <IP_address>
end
```

2. Setting the IPsec phase one to assign IP addresses using the DHCP proxy.

```
config vpn ipsec phase1
   edit <id>
      set assign-ip-from dhcp
   end
end
```

IP assignment can also come from a locally defined range or via the user group.

Transform Matching

FortiOS 5.2 supports combining multiple encryption, authentication, PRF, and DH transforms in a single IKEv2 proposal, which is used for selecting a transform set when the FortiGate unit is the responder. Each proposal now holds lists of transforms, instead of having just a single value per transform type. When negotiating, the proposal iterates over the transform lists to find a match.

Cookie Notification

Upon detecting that the number of half-open IKEv2 SAs is above the threshold value, the VPN dialup server will require all future SA_INIT requests to include a valid cookie notification payload that the server sends back, in order to preserve CPU and memory resources.

Assign Client IP Addresses Using DHCP Proxy

IKE can now use the system DHCP proxy to assign client IP addresses. To use this feature, the DHCP proxy must be enabled and a IP range selected. Up to 8 addresses can be selected for either IPv4 or IPv6. After the DHCP proxy has been configured, the `assign-up-from` command is used to select assign IP address via DHCP.

Syntax

```
system settings
   set dhcp-proxy enable
   set dhcp-server-ip <range>
   set dhcp6-server-ip <range>
end

config vpn ipsec phase1
   set assign-ip-from dhcp
end
```

IP assignment can also come from a locally defined range or via the user group.

IKEv1 Mesh Selectors

IKEv1 mesh selectors are used with IKEv1 static configurations with the phase2 using address group name selectors. When the mesh selector type is set to either host or subnet, and a phase2 is configured with multiple source and destination addresses, this configuration acts as the template selector.

When traffic hits the tunnel in host mode, a dynamic selector is installed for the specific source and destination IP addresses of that packet. When traffic hits the tunnel in subnet mode, a dynamic selector is installed for the specific address of the address group that matched the packet.

These dynamic selectors are not saved to the configuration and will be removed when tunnels are flushed.

Syntax

```
config vpn ipsec phase1-interface
  edit <name>
    set mesh-selector-type {disable | subnet | host}
  end
end
```

Message ID Sync for High Availability

IKE Message ID Sync is supported in FortiOS 5.2. Message ID Sync allows IKEv2 to re-negotiate send and receive message ID counters after a high availability fail over. By doing this, the established IKE SA can remain up, instead of re-initializing.

A diagnose command has also been added to show statistics for the number of HA messages sent/received for IKE: `diagnose vpn ike ha stats`.

Dynamic IPsec Route Control

Greater control has been added in FortiOS 5.2 concerning adding routes for IPsec VPN.

add-route

The `add-route` option is now available for all dynamic IPsec phase 1s and phase 2s, for both policy-based and route-base IPsec VPNs. This allows you to control the addition of a route to a peer destination selector.

This option was previously only available when `mode-cfg` was enabled in phase 1. Also, in phase 2, a new option has been added allowing `add-route` to automatically match the settings in phase 1.

This feature is enabled by default.

Syntax

1. Configuring phase 1:

```
config vpn ipsec {phase1 | phase1-interface}
  edit <name>
    set type dynamic
    set add-route {enable | disable}
  end
end
```

2. Configuring phase 2:

```
config vpn ipsec {phase2 | phase2-interface}
  edit <name>
    set add-route {phase1 | enable | disable}
  end
end
```

Blocking IPsec SA Negotiation

For interface-based IPsec, IPsec SA negotiation blocking can only be removed if the peer offers a wildcard selector. If a wildcard selector is offered then the wildcard route will be added to the routing information base with the distance/priority value configured in the phase1 and, if that is the route with the lowest distance, it will be installed into the forwarding information base.

In a case where this occurs, it is important to ensure that the distance value on the phase1 is set appropriately.

Default Lifetimes and Proposal Values

The default lifetimes for IKE and IPsec have been lengthened in FortiOS 5.2. The number of proposals has also increased and new default proposals have been created for Phase 1 and Phase 2. The changes are as follows:

- The default Phase1 lifetime is 86400 seconds (1 day).
- The default Phase2 lifetime is 43200 seconds (12 hours).
- The default Phase1 proposals are: aes128-sha256, aes256-sha256, 3des-sha256, aes128-sha1, aes256-sha1, and 3des-sha1.
- The default Phase2 proposals are: aes128-sha1, aes256-sha1, 3des-sha1, aes128-sha256, aes256-sha256, and 3des-sha256.
- The maximum number of proposals has been increased from 3 to 10.
- The default Diffie-Hellman (DH) group for phase1 and phase2 has changed from 5 to 14.

Prioritizing DH Group Configuration

In FOS 5.2, the default Diffie-Hellman DH group has changed from 5 to 14, to provide sufficient protection for stronger cipher suites that include AES and SHA2. Because of this change, both IKEv1 and IKEv2 now allow up to 3 DH groups to be configured in the phase 1 and phase 2 settings, while preserving the ordering since the initiator always begins by using the first group in the list. The default DH group in the configuration has been updated to include group 14 and 5, in that order. You can add and remove other groups and the order they appear in the configuration is the order in which they are negotiated.

The IKEv1 protocol does not natively provide for DH group negotiation in Aggressive Mode and Quick Mode. As a result, when multiple DH groups are used with IKEv1 Aggressive Mode or Quick Mode, delays in tunnel establishment can occur and so it is recommended to continue to configure matching DH groups on both peers whenever possible.

During negotiation with multiple DH groups, the new operation is as follows:

1. **IKEv1 Aggressive Mode Initiator:** Since Aggressive Mode includes the KE payload in the first message, FortiOS must select a group to use to generate the DH public number. FortiOS starts with the first group in the list. If the negotiation fails due to timeout, it will try the second group, and finally the third. If the third also fails, FortiOS goes back to the first DH group again, and starts over. Once it finds the correct group and the tunnel is

established, it will continue to use that group for re-keying as long as the VPN connection remains up.

2. **IKEv1 Aggressive Mode Responder:** If the group proposed by the initiator doesn't match the group proposed by the responder, the negotiation fails due to no proposal chosen. Since authentication has not been established the responder cannot send a notify message to the initiator. The initiator will try the next DH group in its configuration when the negotiation time out occurs, which takes 30 seconds by default. At that point, if the next DH group is a successful match, the tunnel comes up.
3. **IKEv1 Main Mode Initiator:** In Main Mode, the SA and KE payloads come in different messages. The SA parameters, including DH group, are negotiated first in MM1 and MM2, then the KE payloads are exchanged in the MM3 and MM4 messages. So no change was made for Main Mode.
4. **IKEv1 Main Mode Responder:** As above, no change for Main Mode.
5. **IKEv1 Quick Mode Initiator:** Quick Mode has the same problem as Aggressive Mode, in that the SA proposal and KE payloads arrive in the same message. So unlike Main Mode, the initiator does not know the negotiated DH group prior to constructing its KE payload. Like with AM, it will start with the first group in the configured DH group list. If the negotiation times out, or if we receive a No-Proposal-Chosen notify message from the responder, we will switch to the next group in the list and try again.
6. **IKEv1 Quick Mode Responder:** Similar to Aggressive Mode, if the initiator's first group doesn't match, the Quick Mode will fail with a no proposal chosen error. In Quick Mode, you have the benefit of an authenticated IKE SA by which you can immediately notify the peer of the error. Sending the No-Proposal-Chosen notify to the initiator allows the initiator to try the next group immediately without waiting for a timeout.
7. **IKEv2 SA_INIT/CHILD_SA Initiator:** Like Aggressive Mode, in IKEv2 both the SA_INIT and CHILD_SA exchanges have the SA proposal and KE payload in the same message. However, unlike IKEv1, the IKEv2 RFC specifies a mechanism to handle this. In IKEv2, if the negotiated DH group does not match the group specified in the KE payload, the INVALID_KE notify message is sent and the initiator retries the exchange using the DH group specified in the notify message. Initiator side support for handling the INVALID_KE message has been added. This code wasn't needed previously, as the IKEv2 CLI allowed only one DH group to be configured. Now that the CLI restriction has been removed and multiple DH groups can be configured for IKEv2 in the phase1 and phase2 settings, the initiator will handle receipt of INVALID_KE messages as per the IKEv2 RFC. As long as the VPN connection remains up, the initiator will subsequently re-key using the negotiated group.
8. **IKEv2 SA_INIT/CHILD_SA Responder:** The responder side of our IKEv2 code already supports handling of the INVALID_KE message.

IPv6 Support for IPsec Phase 2

IPv6 support has been added to IPsec phase 2, allowing IPv6 firewall address and address groups to be used for phase 2 source and destination address types. The management of static selector rules has also been moved into the IKE daemon, allowing named selectors to be reloaded if any named address or address groups are changed, without requiring the FortiGate unit to be rebooted before changes are applied.

IPsec VPN Support with the FortiController-5103B

The FortiController-5103B can now learn the routing table as a slave to receive the update from master. When packets are received, the 5103B blade tests the routing table to determine whether the traffic will be routed to the IPsec interface, if it does, it will trigger 5103 to forward the traffic to dedicated IPsec blade. This ensures that all IPsec traffic is sent to the dedicated

IPsec blade, even traffic originating from the 5000 system, such as monitoring systems or internal emails.

SSL VPN

New SSL VPN features include:

- SSL VPN Configuration
- ECDSA Local Certificates
- Host Security Check Error Replacement Message

SSL VPN Configuration

Several changes have been made to how SSL VPNs are created and configured.

VPN Settings

The SSL VPN settings page, found at *VPN* > *SSL* > *Settings*, has been reorganized to be more intuitive. The settings are now found in the following sections:

- **Connection Settings** define how users connect and interact with an SSL VPN portal. This section includes Listen on Interface(s), Idle Logout, and Server Certificate.
- **Tunnel Mode Client Settings** define the settings that clients will receive upon connecting to the VPN. This section includes Address Range and Allow Endpoint Registration.
- **Authentication/Portal Mapping** allows you to define different portals to different users and groups.

VPN Portal

New options for split tunneling have been added to SSL VPN portals, which are configured by going to *VPN* > *SSL* > *Portals,* including a routing address and a tunnel mode for IPv6. These options can also be configured in the CLI, using the command `config vpn ssl web portal`.

Creating the Firewall Policy

When creating a firewall policy for your SSL VPN, you will select ssl.root as the *Incoming Interface*. Also, source devices are not applicable to SSL VPN firewall policies.

For more information about using a virtual WAN link, please see the FortiGate Cookbook recipe *Providing remote users with access using SSL VPN*, found at docs.fortinet.com.

ECDSA Local Certificates

The use of ECDSA Local Certificates for SSL VPN Suite B support is now supported. This will allow the following:

1. Importing ECDSA certificate.
2. Generating ECDSA certificate requests.
3. Using ECDSA certificate in SSL VPN.
4. Using ECDSA certificate in web-based manager.

ECDSA certificates can be generating using the following command in the CLI: `exec vpn certificate local generate ec`.

RSA certificates are now generated using the command `exec vpn certificate local generate rsa`.

Host Security Check Error Replacement Message

The replacement message that now appears when an SSL VPN host security check fails can now be customized using the CLI.

Syntax

```
config system replacemsg sslvpn hostcheck-error
   set buffer <string>
   set header {none | http | 8bit}
   set format {none | text | html}
end
```

Authentication

New authentication features include:

- Captive Portal
- User Authentication via a POP3 Server
- Limiting Guest User Accounts
- Nested Group Search in LDAP Authentication
- Password Length for User Authentication
- Certificates for Policy Authentication
- Authentication Blackouts
- Single Sign-On for Guest Accounts

Captive Portal

There have been several changes made to authentication using a captive portal.

Additional captive portal options have also been added for wireless networks. For more information, see “Captive Portal for WiFi” on page 96.

External Captive Portals

An external captive portal can be used to configure each FortiGate interface as an independent, external web URL. To configure an interface, go to *System* > *Network* > *Interfaces* and edit the desired interface. Select *Captive Portal* as the *Security Mode*, then set *Authentication Portal* to *External* and configure the other settings as required.

Once a client has been authenticated by the portal, by default they will be sent to original URL that was requested. The portal can also be configured to send the client to a hard coded URL that contains a replacement message.

Syntax

In the following example, the LAN interface is configured with external captive portal that has a specified URL (http://10.6.2.218/?Auth=Success) to redirect clients to after successful authentication.

```
config system interface
  edit "lan"
    set security-mode captive-portal
    set security-external-web "http://10.6.2.218/portal"
    set security-redirect-url "http://10.6.2.218/?Auth=Success"
    set security-groups "rug1"
  end
end
```

Using Groups from the Security Policy

Portal interfaces can now be configured to use the user groups set in the security policies. This will happen by default if no user group is configured on the interface.

Exempting a Policy

Security policies can now be exempt from captive portals, using the command `captive-portal-exempt enable`.

Replacement Messages

The captive portal-specific replacement messages have been removed. Authentication replacement messages will be used for portals.

User Authentication via a POP3 Server

A POP3 server can now be used to verify user credentials when they authenticate through a web portal or any supported authentication method.

The following maximum values are associated with POP3 authentication:

1. A maximum of 10 pop3/pop3s servers can be defined per box
2. A single user group can have up to a pool of 6 POP3 servers assigned

POP3 authentication can be configured using the CLI:

Configuring a POP3 user

```
config user pop3
  edit name
    set server "pop3.fortinet.com"
    set secure {starttls | pop3s | none}
    set port 110
  end
end
```

Configuring a POP3 user group

```
config user group
  edit pop3_grp1
    set member "pop3_server1" "pop3_server2"
  end
end
```

Limiting Guest User Accounts

A new option to has been added to the guest user group where the administrator can restrict the maximum number of guest accounts that can be created. After the limit is reached, the portal administrator will need to remove some expired accounts. The number of accounts can be set from 1-1024 or left as unlimited (0 in the CLI), which is the default setting.

In the web-based manager, the lower limit is restricted if there are existing group members. In order to set a lower number, guest accounts must be removed prior to the limit being set.

Syntax

```
config user group
  edit guest-group
    set group-type guest
    set max-accounts [0-1024]
  end
end
```

Nested Group Search in LDAP Authentication

Nested group search is a new feature added to Windows AD server when the LDAP server's settings have `group-member-check` set to `user-attr`. After authentication succeeds, `fnbamd` gets groups from user attributes and repeats LDAP queries on the groups until reaches the top layer.

Syntax

```
config user ldap
  set search-type nested
end
```

Password Length for User Authentication

In FortiOS 5.2, the length for all passwords connected to user authentication features has been changed to support a maximum of 128 characters.

Certificates for Policy Authentication

The CA certificate used for policy authentication can now be configured, instead of being restricted to the built-in Fortinet certificate. By doing this, the authenticated user can be presented with a certificate that is already trusted by their browser and certificate errors can be avoided.

Syntax

```
config user setting
  set auth-ca-cert <name>
end
```

Authentication Blackouts

If five failed logins are made from an IP within one minute, the IP is put on a blackout list. Future logins from this IP are rejected as long as the IP is on this list. The IP remains on the blackout list for auth-blackout-time seconds.

The amount of time an IP is blacklisted can be configured through the CLI:

Syntax

```
config user setting
  set auth-blackout-time 300
end
```

This feature only applies to IP-based authentication schemes.

Single Sign-On for Guest Accounts

The default *FSSO_Guest_Users* group has changed to *SSO_Guest_Users*. This group supports guests using both Fortinet Single Sign-On (FSSO) and RADIUS Single Sign-On (RSSO).

Users can also now be added to this group SSO_Guest_group using the CLI.

Syntax

```
config user group
  edit SSO_Guest_group
    set member <names>
  end
end
```

Managing Devices

New device management features include:

On-Net Status for FortiClient Devices

The *Online* column of the FortiClient Monitor has been changed to *Status*. This column will show the current status of the device, and whether or not it is registered.

Two of the possible status options are on-net or off-net. In order to record this information, the DHCP server must be enabled for FortiClient On-Net Status. In order to determine if a FortiClient device is on or off net, a DHCP cookie is sent to FortiClient that contains the FortiGate's serial number. FortiClient will then compare that serial number to the number for the FortiGate it is registered with. If they match, the FortiClient will be considered on-net.

In configurations using high availability, the cookie contains the serial number of all cluster members.

This status has also led to the following options have been added to FortiClient profiles:

- Client Web Filtering when On-Net: when enabled, web filtering is applied to FortiClient traffic even when it is protected by a FortiGate unit.
- Auto-connect when Off-Net: This option allows the FortiClient to autoconnect to a VPN even when it has an off-net status.
- Client-based Logging when On-Net: when enabled, the FortiClient will continue to log even when its traffic is flowing through a FortiGate unit.

Endpoint Licenses

New Endpoint licenses are now available in FortiOS 5.2. Information about the status of the current license can be found in the FortiClient section of the *License Information* widget.

The following licenses will be available:

- **Desktop models and FortiGate-VM00:** 200 clients
- **1U models, FortiGate-VM01 and FortiGate-VM02:** 2,000 clients
- **2U models and FortiGate-VM04:** 8,000 clients
- **3U models, FortiGate-ATCA, and FortiGate-VM08:** 20,000 clients

Because the new licenses are for one year, the activation method has changed. New licenses are purchased similarly to a FortiGuard service, with no further registration of the license required. The device can then be registered with the FortiGate unit.

If the device does not have access to Internet, you can download the license key from support site and manually upload it to your FortiGate. The license will be for that specific device and will have an license expiry date.

While the older licenses from FortiOS 5.0 will still be supported, they will have the following limitations:

- The On-Net Status feature will not be supported.
- Logging options will only appear in the CLI.
- FortiAnalyzer Support for logging and reporting will be limited.
- You will not be able to enter any v5.0 license keys.

URL Filter Lists in Endpoint Control

URL filters can now be sent to devices running FortiClient that connect to the FortiGate unit. All URL filter types (Simple/Regex/Wildcard) and actions (Allow/Block/Exempt/Monitor) can be deployed to FortiClient

Upon receiving the URL filter list, FortiClient will save and display the received URL filter list in the web-based manager.

If the URL list is later changed or removed from the FortiGate unit, these changes will also appear in FortiClient.

FortiGuard Categories Consistency with FortiClient

If FortiGuard categories are disabled on a FortiGate unit, they will now also be disabled in FortiClient for managed devices, even if FortiGuard categories were used previously.

Default Device Groups

The predefined device groups have been changed to the following:

- Windows PC (includes Windows servers and computers but not tablets or phones)
- Mac
- Linux
- Printer
- Mobile devices (includes tablets and phones from all vendors)
- VoIP phones
- Router/firewall/gateway devices (does not include switch devices)
- Other (for unknown devices)

To improve accuracy, device types are now identified using UIDs instead of MAC addresses.

Device Detection for Traffic Not Flowing Through the FortiGate

In FortiOS 5.2, any traffic hitting a FortiGate interface, regardless of whether it is going to be dropped, forwarded or processed locally, will be used by device detection, allowing devices to be detected even if their traffic does not flow through the FortiGate unit. This includes traffic that hits an interface with IPS sniffer mode enabled, as well as broadcast and multicast traffic.

Wireless Networking

New wireless networking features include:

- FortiAP Management
- Captive Portal for WiFi
- New Wireless Health Charts
- RADIUS Accounting
- 802.11ac and DARRP Support
- Date Channel DTLS in Kernel

FortiAP Management

How FortiAP units are managed by a FortiGate unit has changed in several ways.

Manually Selecting AP Profiles

AP profiles are no longer assigned automatically. Instead, a default or custom profile must be chosen when the connection to the FortiAP unit is configured.

The *Background Scan* option has also been replaced by *Spectrum Analysis* (for more information, see "New Wireless Health Charts" on page 97) and either 20MHz or 40MHz must be selected for Radio 1's channel width.

You can choose to override some options set in the profile for a particular FortiAP unit. To do this, go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAPs* and, under *Wireless Settings*, select *Override Settings*. This allows you to change WiFi radio settings, including SSIDs, TX power, and rogue AP scanning. This can also be configured in the CLI:

Syntax

```
config wireless-controller wtp
  edit <name>
    set override-profile enable
  end
end
```

AP Scanning

AP scanning, including rogue AP detection, is now part of WIDS Profiles. It can be found by going to *WiFi Controller* > *WiFi Network* > *WIDS Profiles*. It can also be configured through the CLI:

Syntax

```
config wireless-controller wids-profile
  edit 0
    set ap-scan {enable | disable}
    set ap-bgscan-period <interval>
    set ap-bgscan-intv <interval>
    set ap-bgscan-duration <interval>
    set ap-bgscan-idle <interval>
    set ap-bgscan-rpot-intv <interval>
    set ap-bgscan-disable-day <day>
    set ap-fgscan-repot-intv <interval>
    set rogue-scan {enable | disable}
  end
end
```

Radio Settings Summary

The Radio Settings Summary table can be found by going to *WiFi Controller* > *Managed Access Points* > *Managed FortiAPs* and editing a FortiAP unit. The table shows information on the FortiAP unit's Radio 1 and 2 (if applicable), including settings, channels, and SSIDs.

CLI Console Access

The CLI console on a FortiGate unit can now be used to connect directly to a managed FortiAP unit that has been configured to enable login-enable. To access the FortiAP, use the command `execute telnet <ip>`, using the IP address of the FortiAP.

Telnet must be used, as FortiAPs do not support SSH/HTTPS admin access.

The console can also now be accessed by going to *WiFi Controller* > *Managed Access Points* > *Managed APs* and selecting the option *Connect to CLI*. The console will appear in a pop-up window.

If `login-enable` is set to `default` or `disable` on the FortiAP unit, or the FortiAP is offline, this option will not appear.

Split Tunneling for Wireless Traffic

Split tunneling can now be used for wireless traffic, allowing you to optimize WiFi traffic flow by directing only corporate traffic back to the FortiGate unit's wireless controller, while local application traffic remains local. With split tunneling, a remote user associates with a single SSID, can get access to corporate resources (for example, a mail server) and local resources (for example, a local printer).

Split tunneling should be only used for SSIDs in tunnel mode.

Syntax

1. Enabling split tunnelling for an SSID.

```
config wireless-controller vap
  edit <name>
    set split-tunneling enable
  end
end
```

2. Setting the IP lists for split tunneling

```
config w-c {wtp-profile | wtp}
  set split-tunneling-acl-local-ap-subnet enable
  config split-tunneling-acl
    edit <ID>
      set id <ID>
      set dest-ip <IP_address>
    end
  end
end
```

Captive Portal for WiFi

Several changes have been made for captive portal security on wireless networks. Wireless captive portals can also use the new features for all captive portals described in "Captive Portal" on page 88.

New Configuration Options

The following options can now be configured for captive portals that use wireless interfaces:

- Security exempt list names can be added to a captive portal. This option is only available when user groups are selected as part of the SSID configuration, rather than being a match for groups in the security policy.
- URL redirection is available after the disclaimer/authentication screen.
- Four types of portals are available: authentication, authentication with disclaimer, disclaimer only, or email collection. When the mode is email collection or disclaimer only, the options for setting user groups or having an external captive portal are not available.

Syntax

```
config wireless-controller vap
  edit <name>
    set security captive-portal
    set portal type {auth | auth+disclaimer | disclaimer |
        email-collect}
    set security-exempt-list <name of list>
  end
end
```

WPA Personal Security + Captive Portal

A new option has also been added that uses WPA Personal security as well as a captive portal. This option also allows groups to be imported from the policy.

New Wireless Health Charts

Two new charts have been added to the Wireless Health Monitor showing spectrum analysis information on the sources of wireless interference.

In order for these widgets to appear, spectrum analysis must first be enabled. This is done by editing the AP profile used by your FortiAP units and selecting *Spectrum Analysis* for all applicable radios.

Spectrum analysis can also be enabled in the CLI.

Syntax

```
config wireless-controller wtp-profile
  edit <name>
    config <radio>
      set spectrum-analysis enable
    end
  end
end
```

After spectrum analysis has been enabled, view the *Top Wireless Interference* widget found in the Wireless Health Monitor. A chart icon will appear in the *Channel* column. Selecting this icon will open the new WiFi charts: *Spectrum Analysis* and *Top Wireless Interference*.

The *Spectrum Analysis* chart shows WiFi signal interference as detected by a particular FortiAP.

The *Top Wireless Interference* chart shows SSIDs that are interfering with a particular FortiAP unit.

RADIUS Accounting

RADIUS accounting is now supported for wireless networks, allowing RADIUS accounting messages to be sent that contain a wireless user's name and IP address.

If an accounting server has been enabled for RADIUS, the wireless client information will be sent to it.

802.11ac and DARRP Support

802.11ac support has been added for FortiOS 5.2, allowing a FortiGate unit to manage FortiAP models 221C and 320C. Distributed Automatic Radio Resource Provisioning (DARRP) is also supported for 802.11ac radio.

Syntax

```
config wireless-controller wtp-profile
  edit {fap221c | fap320c}
    config radio-2
      set darrp enable
    end
  end
end
```

Date Channel DTLS in Kernel

Data channel Datagram Transport Layer Security (DTLS) can now be enabled in kernel using the CLI.

Syntax

config wireless-controller wtp-prof

```
    edit wtpprof
      set dtls-in-kernel enable
    end
  end
```

IPv6

New IPv6 features include:

- IPv6 Address Ranges
- TCP MSS Values
- RSSO Support
- FortiManager Connections
- Geographical Database

IPv6 Address Ranges

IPv6 address ranges can now be created, using either the web-based manager or the CLI.

Syntax

```
config firewall address6
  edit <name>
    set type iprange
    set start-ip <address>
    set end-ip <address>
  end
end
```

TCP MSS Values

TCP MSS values for both the sender and the receiver can now be set for IPv6 policies using the CLI.

Syntax

```
config firewall policy6
  edit <index_int>
    set tcp-mss-sender <value>
    set tcp-mss-receiver <value>
  end
end
```

RSSO Support

RADIUS Single Sign-On (RSSO) is supported in IPv6 and can be configured in the CLI. Fallthrough for unauthenticated

Syntax

```
config firewall policy6
  edit <id>
    set rsso enable
    set fall-through-unauthenticated enable
  end
end
```

FortiManager Connections

IPv6 can now be used to connect a FortiGate unit to a FortiManager unit.

Geographical Database

An IPv6 geographical database has been added to properly identify the geographical locations of traffic in reports.

High Availability

New high availability features include:

- DHCP and PPPOE Support for Active-Passive Mode
- VRRP Support
- Trigger Failover
- Synchronizing a GTP Tunnel over Physical Ports
- IPv6 Management Interface Gateway

DHCP and PPPOE Support for Active-Passive Mode

High Availability is now supported in Active-Passive mode when there are interfaces working in DHCP client or PPPOE client mode.

VRRP Support

Additional features have been added to support Virtual Router Redundancy Protocol (VRRP).

VRRP Groups

A VRRP group includes all the relevant VRRP IDs and tracks the VRRP status in order to force the status of all group members if a VRRP domain is changed from master to backup.

VRRP groups are configured through the CLI. The VRRP group ID can be between 1 and 65535.

Syntax

```
config system interface
  edit <port>
    config vrrp
      edit <id>
        set vrgrp <id>
      end
    end
  end
end
```

A *VRRP* column has also been added to the interfaces list in the web-based manager that will show the VRRP ID, group, and status. This list can be found at *System* > *Network* > *Interfaces*.

Using a Second Destination IP (VRDST)

VRRP can now be configured with second destination IP (VRDST) for monitoring. When two IPs are used, VRRP failure will only be reported if both monitored IPs are down.

A second VRDST can be configured using the CLI.

Syntax

```
config system interface
   edit <interface>
      config vrrp
         edit <id>
            set vrdst <ip1> <ip2>
         end
      end
   end
end
```

Trigger Failover

HA failover can now be enabled and disabled using the following CLI commands:

- `diagnose sys ha set-as-master enable`: immediately enables the local FortiGate unit as the HA master.
- `diagnose sys ha set-as-master disable`: immediately disables this mode. Optionally, a time frame can be added after `disable`, which will disable the mode at the appointed time. The time format is yyyy-mm-dd hh:mm:ss.

Synchronizing a GTP Tunnel over Physical Ports

In order to properly handle GPRS Tunneling Protocol (GTP) synchronization under high stress loads, FortiOS 5.2 will use the interfaces set in `set session-sync-dev` (part of `config system ha`) to allow GTP tunnels to be synchronized directly over physical ports when both the HA primary and secondary are up.

A new diagnose command, `diagnose firewall gtp hash-stat`, has also been added to display GTP hash stat separately.

IPv6 Management Interface Gateway

IPv6 management interface gateways are now supported in FortiOS 5.2.

Syntax

```
config system ha
   set ha-mgmt-interface-gateway6 <IPv6_address>
end
```

WAN Optimization, Web Cache, and Explicit Proxy

New WAN optimization, web cache, and explicit proxy features include:

- Explicit Proxy Policy Table - for explicit web proxy, explicit FTP proxy and WAN optimization policies
- Distributing Explicit Web Proxy Traffic to Multiple CPU Cores
- Proxy Header Control
- Explicit Web Proxy SOCKS services support for TCP and UDP traffic
- Preventing the explicit web proxy from changing source addresses
- Explicit web proxy firewall address URL patterns

Explicit Proxy Policy Table - for explicit web proxy, explicit FTP proxy and WAN optimization policies

Explicit proxy polices now have a dedicated table and creation page, found at *Policy & Objects* > *Policy* > *Explicit Proxy*. The corresponding CLI command is:

```
config firewall explicit-proxy-policy
```

You use explict proxy policies to add policies for the IPv4 and IPv6 explicit web proxy and for the explicit FTP policy. The first step in creating an explicit proxy policy is to select the proxy type (web or FTP). The options availabl e then depend on the explicit proxy type.

From the CLI you use the explicit web proxy policy to add WAN optimization tunnel policies. In FortiOS 5.0 you added WAN optimization tunnel policies by setting the source interface to wanopt. In FortiOS 5.2 you create an explicit web proxy policy from the CLI and set the proxy type to wanopt. For example:

```
configure firewall explicit-proxy-policy
  edit 0
    set proxy wanopt
    set dstintf internal
    set srcaddr all
    set dstaddr server-subnet
    set action accept
    set schedule always
    set service ALL
  next
end
```

Distributing Explicit Web Proxy Traffic to Multiple CPU Cores

To improve explicit web proxy performance, FortiOS 5.2 distributes explicit web proxy processing to multiple CPU cores. By default web proxy traffic is handled by half of the CPU cores in a FortiGate unit, so if your FortiGate unit has 4 CPU cores, by default two will be used for explicit web proxy traffic. You can increase or decrease the number of CPU cores that are used in the CLI.

```
config system global
  set wad-worker-count <number>
end
```

The value for `<number>` can be anything between 1 and the total number of CPU cores in your FortiGate unit. The default value for `<number>` is half the number of CPU cores in your FortiGate unit.

Proxy Header Control

You can create explicit web proxy profiles that can add, remove and change HTTP headers. The explicit web proxy profile can be added to a web explicit proxy policy and will be applied to all of the HTTP traffic accepted by that policy.

You can change the following HTTP headers:

- client-ip
- via header for forwarded requests
- via header for forwarded responses
- x-forwarded-for
- front-end-https

For each of these headers you can set the action to:

- Pass to forward the traffic without changing the header
- Add to add the header
- Remove to remove the header

You can also configure how the explicit web proxy handles custom headers. The proxy can add or remove custom headers from requests or responses. If you are adding a header you can specify the content to be included in the added header.

Create web proxy profiles from the CLI:

```
config web-proxy profile
  edit <name>
    set header-client-ip {add | pass | remove}
    set header-via-request {add | pass | remove}
    set header-via-response {add | pass | remove}
    set header-x-forwarded-for {add | pass | remove}
    set header-front-end-https {add | pass | remove}
      config headers
        edit <id>
          set action {add-to-request | add-to-response |
              remove-from-request | remove-from-response}
          set content <string>
          set name <name>
        end
  end
```

Use the following command to add a web proxy profile to an explicit proxy policy:

```
config firewall explicit-proxy-policy
  edit <id>
    set webproxy-profile <name>
  end
```

Explicit Web Proxy SOCKS services support for TCP and UDP traffic

You can now configure Web Proxy services to allow UDP traffic as well as TCP traffic to be accepted by the SOCKS proxy. Previously, the web proxy would only accept TCP SOCKS traffic.

Web proxy services can be configured in the CLI.

Syntax

Use the following command to create a custom service for UDP traffic over the SOCKS proxy:

```
config firewall service custom
  edit <name>
    set explicit-proxy enable
    set category Web\ Proxy
    set protocol SOCKS-UDP
    set tcp-portrange 8080-8080
  end
end
```

The option to create a custom service for TCP traffic over the SOCKS proxy has also changed. For example, use the following command to create a custom service for TCP traffic over the SOCKS proxy:

```
config firewall service custom
  edit <name>
    set explicit-proxy enable
    set category Web\ Proxy
    set protocol SOCKS-TCP
    set tcp-portrange 80-80
  end
end
```

Preventing the explicit web proxy from changing source addresses

By default in NAT/Route mode the explicit web proxy changes the source address of packets leaving the FortiGate to the IP address of the FortiGate interface that the packets are exiting from. In Transparent mode the source address is changed to the management IP.

This configuration hides the IP addresses of clients and allows packets to return to the FortiGate unit interface without having to route packets from clients. You can use the following command to configure the explicit web proxy to keep the original client's source IP address:

```
config firewall explicit-proxy-policy
  edit 0
    set proxy web
    set transparent enable
  end
```

Explicit web proxy firewall address URL patterns

You can add URL pattern addresses and address groups to control the destination URLs that explicit web proxy users can connect to. To add a URL pattern to go to *Policy & Objects* > *Objects* > *Addresses*, select *Create New* and set the Type to *URL Pattern (Explicit Proxy)*. Add a URL or URL pattern that defines the URL or URLs that explicit proxy users should be limited to. Set the *Interface* to *any*.

For example to limit access to a single website:

www.fortinet.com

To limit access to websites from the same domain:

google.com

To limit access to a part of a website:

www.apple.com/ipad/

To add a URL pattern group, create several URL pattern addresses then go to *Policy & Objects* > *Objects* > *Addresses*, select *Create New* > *Group* and add URL patterns to the address group.

Then when creating explicit web proxy policies, select the URL pattern addresses or groups as the destination address.

URL patterns and HTTPS scanning

For HTTPS traffic, URL patterns can only be matched up to the root path. For example, consider the following URL pattern:

www.apple.com/ipad/

If a proxy user browses using HTTP, this URL pattern limits their access the iPad pages of www.apple.com. However, if a proxy user browses using HTTPS, they will be able to access all pages on www.apple.com.

Advanced Routing

New advanced routing features include:

- BGP Neighbor Groups
- OSPF Fast Hello
- BGP Conditional Advertising
- Source and Destination IP-based Mode for ECMP
- Policy Routes

BGP Neighbor Groups

A Border Gateway Protocol (BGP) neighbor group can now be configured automatically based on a range of neighbors' source addresses, rather than configuring neighbors individually. A maximum number of neighbors can be set for each group to be between 1 and 1000.

Syntax

```
config router bgp
   config neighbor-group
      edit <name>
         set ... (same configuration options as config neighbor)
   next
   config neighbor-range
      edit <id>
         set prefix <class_ip&net_netmask>
         set max-neighbor-num <integer>
         set neighbor-group <name>
      end
   end
end
```

OSPF Fast Hello

Open Shortest Path First (OSPF) fast hello provides a way to send a set number of hello packets per second and use a dead interval of four hellos. Fast hello can be configured on an OSPF interface through the CLI. If `dead-interval` is set to 1 second, fast hello will be enabled. The `hello-multiplier` value, which can be between 4 and 10, sets the number of hello packets that will be sent per second.

Syntax

```
config ospf-interface
  edit ospf1
    set interface port1
    set network-type broadcast
    set dead-interval 1
    set hello-multiplier 4
  end
end
```

BGP Conditional Advertising

BGP conditional advertising is supported in FortiOS 5.2.

Normally, routes are propagated regardless of the existence of a different path. Using BGP conditional advertisement allows a route not to be advertised based on existence or non-existence of other routes. With this new feature, a child table under bgp neighbor is introduced. Any route matched by one of the route-map specified in the table will be advertised to the peer based on the corresponding condition route-map.

Syntax

```
config router bgp
  config neighbor
    edit <name>
      set remote-as 3
      config conditional-advertise
        edit <name>
          set condition-routemap <name>
          set condition-type {exist | non-exist}
        end
      end
    end
  end
end
```

Source and Destination IP-based Mode for ECMP

A new mode has been added that allows Equal-cost multi-path routing (ECMP) to select next hop based on both source and destination IPs. This can be configured as a global setting (if `virtual-wan-link` is disabled) or for a virtual WAN link.

Syntax

```
config system {settings | virtual-wan-link}
  set v4-ecmp-mode source-dest-ip-based
end
```

Policy Routes

The following options have been added for policy routes:

- Multiple source/destination subnets.
- Multiple input devices.
- `src-negate` and `dst-negate` can now be enabled.
- `action` can now be set to `permit` or `deny`.

Logging and Reporting

New logging and reporting features include:

Traffic and UTM Logging Improvements

Traffic and UTM Logging has been simplified in FortiOS 5.2 by making the following changes:

- Removing all overlapping fields between the UTM Logs and Traffic Logs, with the exception of the common fields `sessionid`, `vd`, `user`, and `group`, and application control critical info, which will be present in both the Traffic Log and Application log.
- Fields have been renamed so that they are the same in all logs.
- Some rarely used fields were removed; for example, `profiletype`.
- The `action` field reflects the Firewall action (accept or deny). This will allow you to see from the traffic logs if the session was allowed or blocked and whether it was allowed or blocked by the firewall or by a security feature. If it was a security feature, you will need to look at the UTM logs to determine which feature blocked the traffic.
- The field `utmaction` is set to the most severe actions across all security features. The severity from highest to lowest is: Block, Reset, Traffic Shape, Allow.
- You can now drill-down from a traffic log to its corresponding UTM logs.
- `extended-utm-log` and `log` options for security profiles have been removed.
- Log roll logic have been rewritten so that traffic log file and related utm log files are rolled together. Uploadd will pack these files together to send to a FortiAnalyzer unit.
- An anomaly log category has been added to separate anomaly logs from IPS logs.

FortiGate Daily Security Report

The FortiGate UTM Security Analysis Report has been renamed the FortiGate Daily Security Report.

A variety of other changes have also occurred to the report:

- A new cover page has been added that contains the report name, date, date range, and device name.
- A table of contents page has been added.
- The information VPN usage now shows all use, rather than just a top 10 list. This allows a complete list to be shown that includes all tunnels for Site-to-Site IPsec VPNs and all users for dial-up IPsec VPN tunnels, SSL VPN tunnels, and SSL VPN web mode. Information on connection time has also been added.
- Entries will not be displayed when there is a zero bandwidth/or connection time.

GTP Logging Improvements

Several changes have been made concerning GPRS Tunneling Protocol (GTP) and logging.

GTP-U Logging

FortiOS 5.2 supports GPRS Tunnelling Protocol User Plane (GTP-U) logging for both forwarded and dropped packets at the kernel level. FortiGate log entries now contain International Mobile Subscriber Identity (IMSI), Mobile Subscriber Integrated Services Digital Network-Number (MSISDN), Access Point Name (APN), and header Tunnel Endpoint Identifier (TEID) if available/applicable.

Three new CLI commands are added to GTP profile for GTP-U logging:

- `gtpu-forwarded-log`: Enable/disable logging of forwarded GTP-U packets.
- `gtpu-denied-log`: Enable/disable logging of denied GTP-U packets.
- `gtpu-log-freq`: Sets the logging frequency of GTP-U packets.

Syntax

```
config firewall gtp
  edit gtp_profile
    set gtpu-forwarded-log enable
    set gtpu-denied-log enable
    set gtpu-log-freq 10
  end
end
```

The log frequency value is per number of packets, for example `set gtpu-log-freq 10` means the FortiGate unit should have a log entry per 10 packets.

GTP Event Log

A new GTP event log has been added, which can be found by going to *Logging & Reports* > *Event Log* > *GTP*. This log will show GTP activity status and a Deny Cause for any traffic that was blocked or dropped.

In order to see this log, it must be enabled either in the Log Settings or in the CLI.

Syntax

```
config log eventfilter
  set gtp enable
end
```

Flash-based Logging Disabled on Some Models

On some FortiGate models, flash-based logging is not available in FortiOS 5.2. For these platforms, Fortinet recommends the free FortiCloud central logging & reporting service, as it offers higher capacity and extends the features available to the FortiGate.

For a full list of affected models, please refer to the *Release Notes*.

Accessing Policy-specific Logs from the Policy List

In FortiOS 5.2, the log viewer can be opened directly from the policy table, with filters applied automatically to show only the logs relating to that policy. To view these logs, right-click on the *Seq.#* column for the policy and select *Show Matching Logs*.

The log viewer will filter using the Policy UUID if it is enabled. If not, the Policy ID will be used.

IPS Event Context Data in Log Messages

Attack context logging can now be enabled for an IPS sensor, which will add two new fields, `attackcontext` and `attackcontextid`, into an attack log.

The `atkctx` field in log will output BASE64 encoded string of:

```
<PATTERNS> trigger patterns separated by ';' </PATTERNS> <URI> uri
     buffer </URI> <HEADER> header buffer </HEADER> <BODY> body
     buffer </BODY> <PACKET> packet buffer </PACKET>"
```

`Attackcontext` entries longer than 1KB is split in multiple log entries, which share the same `incidentserialno`. `Attackcontextid` will help identify these segment by showing what order they have in the sequence; for example, `<1/3>` means this log is the first segment of a log message containing three segments in total.

Sniffer Traffic Log

Forward traffic from a FortiGate unit that is in one-arm sniffer mode can now be logged on that FortiGate unit. To log this traffic, the appropriate logging option must be selected for the sniffer interface.

Logging information can be viewed in the new sniffer log, which can be found by going to *Log & Report* > *Forward Traffic* > *Sniffer Traffic*.

Selecting Sources for Reports

The source for reports can now be configured to be either forward traffic, sniffer traffic, or both.

Syntax

```
config report setting
   set status enable
   set report-source {forward-traffic | sniffer-traffic | both}
end
```

Threat Weight

The 5.0 feature client reputation has been renamed Threat Weight in FortiOS 5.2 and has been moved from Security Profiles to *Log & Report* > *Log Config* > *Threat Weight*. It can now be configured in the CLI using the command `config log threat-weight`.

Disk Usage Information in System Event Logs

Disk usage information will now be included in system event logs for FortiGate models that have a hard disk.

Event Log Generated When a Crash Occurs

A brief event log will now be generated when a crash occurs with brief information about the crash.

Displaying FortiFlow Names

Object name data will now be pulled from FortiFlow in applicable locations, including the *Forward Traffic* log and the *Top Destinations* widget.

Other New Features

Other new features in FortiOS 5.2 include:

SIP Traffic is Handled by the SIP ALG by Default

Previous versions of FortiOS used the SIP session helper for all SIP sessions. You had to remove the SIP session helper from the configuration for SIP traffic to use the SIP ALG.

In FortiOS 5.2, all SIP traffic is now processed by the SIP ALG by default. You can change the default setting using the following command:

```
config system settings
  set default-voip-alg-mode {proxy-based | kernel-helper-based}
end
```

The default is `proxy-based`, which means the SIP ALG is used. If set to `kernel-helper-based`, the SIP session helper is used. If a SIP session is accepted by a firewall policy with a VoIP profile, the session is processed using the SIP ALG even if `default-voip-alg-mode` is set to `kernel-helper-based`.

If a SIP session is accepted by a firewall policy that does not include a VoIP profile:

- If `default-voip-alg-mode` is set to `proxy-based`, SIP traffic is processed by the SIP ALG using the default VoIP profile.
- If `default-voip-alg-mode` is set to `kernel-helper-based`, SIP traffic is processed by the SIP session helper. If the SIP session help has been removed, then no SIP processing takes place.

Changing the Header Name of Load Balanced HTTP/HTTPS Traffic

A header name can now be configured for HTTP and HTTPS traffic that flows through a virtual server, rather than using the default X-Forward-For header.

In order to use this feature, the HTTP IP header must be enabled.

Syntax

```
config firewall vip
  edit <name>
    set type server-load-balance
    set server-type {http | https}
    set http-ip-header enable
    set http-ip-header-name <name>
  end
end
```

TOS and DSCP Support for Traffic Mapping

Both TOS and DSCP are now supported for traffic mapping but only one method can be used at a time, with TOS as the default. The type used and its other attributes can be configured through the CLI.

Syntax

```
config system global
   set traffic-priority {tos | dscp}
   set traffic-priority-level {low | medium | high}
end
```

RFC List

The following RFCs are supported by the new features in FortiOS 5.2

Number	Title
791	Internet Protocol
1349	Type of Service in the Internet Protocol Suite
1925	The Twelve Networking Truths
2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
4754	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
4787	Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
5996	Internet Key Exchange Protocol Version 2 (IKEv2)